

# **Exhibit 1**

## Supreme Court of Pennsylvania

Court of Common Pleas

Civil Cover Sheet

Lebanon

County

For Prothonotary Use Only:

Docket No:

10696-19

TIME STAMP

The information collected on this form is used solely for court administration purposes. This form does not supplement or replace the filing and service of pleadings or other papers as required by law or rules of court.

## Commencement of Action:

- ☒ Complaint
 ☐ Writ of Summons
 ☐ Petition
 ☐ Declaration of Taking
 ☐ Transfer from Another Jurisdiction

Lead Plaintiff's Name:  
First Choice Federal Credit Union

Lead Defendant's Name:  
Equifax, Inc.

Are money damages requested? ☒ Yes ☐ No

Dollar Amount Requested: ☐ within arbitration limits  
(check one) ☒ outside arbitration limits

Is this a Class Action Suit? ☒ Yes ☐ No

Is this an MDJ Appeal? ☐ Yes ☒ No

Name of Plaintiff/Appellant's Attorney: Gary F. Lynch, Carlson Lynch LLP

☐ Check here if you have no attorney (are a Self-Represented [Pro Se] Litigant)

**Nature of the Case:** Place an "X" to the left of the ONE case category that most accurately describes your **PRIMARY CASE**. If you are making more than one type of claim, check the one that you consider most important.

## TORT (do not include Mass Tort)

- ☐ Intentional  
☐ Malicious Prosecution  
☐ Motor Vehicle  
☐ Nuisance  
☐ Premises Liability  
☐ Product Liability (does not include mass tort)  
☐ Slander/Libel/ Defamation  
☒ Other:  
 Data Breach

## MASS TORT

- ☐ Asbestos  
☐ Tobacco  
☐ Toxic Tort - DES  
☐ Toxic Tort - Implant  
☐ Toxic Waste  
☐ Other:

## PROFESSIONAL LIABILITY

- ☐ Dental  
☐ Legal  
☐ Medical  
☐ Other Professional:

## CONTRACT (do not include Judgments)

- ☐ Buyer Plaintiff  
☐ Debt Collection: Credit Card  
☐ Debt Collection: Other

- ☐ Employment Dispute:  
 Discrimination  
☐ Employment Dispute: Other

☐ Other:

## CIVIL APPEALS

- Administrative Agencies  
☐ Board of Assessment  
☐ Board of Elections  
☐ Dept. of Transportation  
☐ Statutory Appeal: Other

☐ Zoning Board

☐ Other:

## REAL PROPERTY

- ☐ Ejectment  
☐ Eminent Domain/Condemnation  
☐ Ground Rent  
☐ Landlord/Tenant Dispute  
☐ Mortgage Foreclosure: Residential  
☐ Mortgage Foreclosure: Commercial  
☐ Partition  
☐ Quiet Title  
☐ Other:

## MISCELLANEOUS

- ☐ Common Law/Statutory Arbitration  
☐ Declaratory Judgment  
☐ Mandamus  
☐ Non-Domestic Relations  
☐ Restraining Order  
☐ Quo Warranto  
☐ Replevin  
☐ Other:

JUL 12 2019

PRO &amp; CLERK

**IN THE COURT OF COMMON PLEAS OF LAWRENCE COUNTY,  
PENNSYLVANIA**

FIRST CHOICE FEDERAL CREDIT  
UNION, individually and on behalf of all  
others similarly situated,

Plaintiff,

v.

EQUIFAX, INC., and EQUIFAX  
INFORMATION SERVICES LLC,

Defendants.

CIVIL DIVISION  
CLASS ACTION

No. 10696-19

**CLASS ACTION COMPLAINT**

FILED ON BEHALF OF PLAINTIFF,  
First Choice Federal Credit Union

COUNSEL OF RECORD FOR THIS  
PARTY:

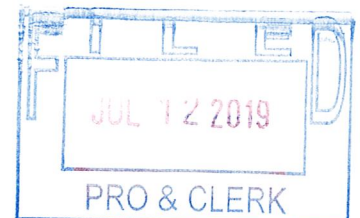
GARY F. LYNCH  
Pa. ID No. 56887  
KELLY K. IVERSON  
Pa. ID No. 307175  
JAMISEN A. ETZEL  
Pa. ID No. 311554

**CARLSON LYNCH LLP**  
1133 Penn Avenue, 5th Floor  
Pittsburgh, Pennsylvania 15222  
Telephone: (412) 322-9243  
Facsimile: (412) 231-0246

*(All to be admitted Pro Hac Vice)*  
JOSEPH P. GUGLIELMO  
ERIN GREEN COMITE

**SCOTT+SCOTT**  
**ATTORNEYS AT LAW LLP**  
230 Park Avenue, 17th Floor  
New York, NY 10169  
Telephone: (212) 223-6444  
Facsimile: (212) 223-6334

**JURY TRIAL DEMANDED**





**IN THE COURT OF COMMON PLEAS OF LAWRENCE COUNTY,  
PENNSYLVANIA**

FIRST CHOICE FEDERAL CREDIT  
UNION, individually and on behalf of all  
others similarly situated,

CIVIL DIVISION

No. \_\_\_\_\_

Plaintiff,

v.

EQUIFAX, INC., and EQUIFAX  
INFORMATION SERVICES LLC,

Defendants.

**NOTICE TO DEFEND**

**YOU HAVE BEEN SUED IN COURT.** If you wish to defend against the claims set forth in the following pages, you must take action within **TWENTY (20)** days after this Complaint and Notice are served, by entering a written appearance personally or by attorney and filing in writing with the court your defenses or objections to the claims set forth against you. You are warned that if you fail to do so the case may proceed without you and a judgment may be entered against you by the court without further notice for any money claimed in the Complaint or for any claim or relief requested by the Plaintiff. You may lose money or property or other rights important to you.

**YOU SHOULD TAKE THIS PAPER TO YOUR LAWYER AT ONCE. IF YOU DO NOT HAVE A LAWYER, GO TO OR TELEPHONE THE OFFICE SET FORTH BELOW TO FIND OUT. THIS OFFICE CAN PROVIDE YOU WITH INFORMATION ABOUT HIRING A LAWYER.**

**IF YOU CANNOT AFFORD TO HIRE A LAWYER, THIS OFFICE MAY BE ABLE TO PROVIDE YOU WITH INFORMATION ABOUT AGENCIES THAT MAY OFFER LEGAL SERVICES TO ELIGIBLE PERSONS AT A REDUCED FEE OR NO FEE.**

LAWRENCE COUNTY LAWYER REFERRAL  
430 Court Street, 3<sup>rd</sup> Floor  
New Castle, PA 16101  
724-656-1921

**IN THE COURT OF COMMON PLEAS OF LAWRENCE COUNTY,  
PENNSYLVANIA**

FIRST CHOICE FEDERAL CREDIT  
UNION, individually and on behalf of all  
others similarly situated,

CIVIL DIVISION

No. \_\_\_\_\_

Plaintiff,

v.

EQUIFAX, INC., and EQUIFAX  
INFORMATION SERVICES LLC,

Defendants.

**CLASS ACTION COMPLAINT**

*“[T]here’s no doubt that securing data is the core value of our company. And I will [] apologize  
deeply to the American public for the breach that we had.  
We let the public down.”*

Richard Smith, Former Chief Executive Officer of Equifax Inc.  
Nov. 8, 2017 Hearing, U.S. Senate Committee on  
Commerce, Science & Transportation

## INTRODUCTION

1. “*Powering the World with Knowledge.*” Equifax serves as a linchpin of the U.S. economy. By aggregating consumer data, Equifax enables financial institutions to extend credit and other financial services to U.S. consumers. Equifax heralds itself as a “trusted steward” that complies with the laws requiring Equifax to adequately safeguard consumer data. In reality, Equifax prioritized profits over privacy, exposing the information it acknowledged was responsible for powering the world.

2. Plaintiff brings this class action to remedy the financial losses they suffered and continue to suffer, as well as the certainly impending risk of future harm that is likely to occur in the form of future fraudulent banking activity as a direct result of Equifax’s egregious negligent mishandling of highly sensitive, personally identifiable information (“PII”).

3. Equifax’s senior management ignored specific warnings that its systems were vulnerable to attack and refused to take the necessary steps to adequately protect consumer data. As a direct result of Equifax’s weak cybersecurity measures, between at least May and July 2017, hackers stole the highly sensitive PII of approximately 147.9 million U.S. consumers – roughly 46% of the U.S. population and nearly 60% of all adults in the U.S. (the “Data Breach”). The Equifax Data Breach is arguably the most damaging data breach in this country’s history, impacting at least one family member in *every* U.S. household. This data was obtained by Equifax from Plaintiff and other financial institutions. This PII includes but is not limited to:

- a. names;
- b. Social Security numbers;
- c. birth dates;
- d. addresses;

- e. driver's license numbers;
- f. images of taxpayer ID cards, passports or passport cards, and other government-issued identification documents;
- g. photographs associated with these forms of government-issued identification; and
- h. payment card data ("Payment Card Data"), including, but not limited to, credit and debit card numbers, primary account numbers ("PANs"), card verification value numbers ("CVVs"), expiration dates, and zip codes.

4. This Data Breach shocks the conscience. Equifax fully understood its duties to protect the confidentiality, accuracy, and integrity of PII. Equifax fully understood that the threat of a data breach was a legitimate risk, and that if one occurred, the consequences would be severe. Yet time and time again, Equifax refused to take the necessary steps to adequately protect consumer data. Indeed, in the months prior to the Data Breach, Equifax was subject to no fewer than five data breach incidents in which PII was compromised. It even received notification of the specific vulnerability that led to the Data Breach.

5. The Equifax Data Breach was a direct consequence of Equifax's deliberate decisions not to adopt recommended data security measures, decisions that left PII vulnerable. Equifax's data security deficiencies were so significant that the hackers' activities went undetected for at least two months. During that time, the hackers had unfettered access to exfiltrate likely hundreds of millions of lines of consumer data. Had Equifax adopted reasonable data security measures, it could have prevented the Data Breach.

6. Equifax's former Chief Executive Officer ("CEO") Richard Smith admitted: "We at Equifax clearly understood that the collection of American consumer information and data

carries with it enormous responsibility to protect that data. We did not live up to that responsibility[.] . . . Equifax was entrusted with Americans' private data and we let them down."<sup>1</sup>

7. Financial institutions, like Plaintiff and the Class, and Equifax have a symbiotic relationship. Equifax relies on the consumer data furnished by Plaintiff and the Class, and Plaintiff and the Class rely on Equifax to provide accurate consumer data enabling them to the full range of financial services that U.S. consumers expect.

8. Equifax knew that if it were to suffer a data breach, the repercussions would extend directly to the financial services industry. The compromised PII is precisely the data needed for identity thieves to wreak havoc throughout the financial services industry, enabling them to illegitimately open accounts, apply for credit and loans, and transfer funds with stolen and synthetic identities.<sup>2</sup>

9. Because the vast quantity of consumer data compromised as a result of the Data Breach is the data Plaintiff and the Class furnished to Equifax and used to conduct their business, Plaintiff and the Class have been injured and are at increased risk of suffering additional losses as a result of various forms of fraudulent banking activity. Indeed, the consequences of the Equifax Data Breach are so massive that Social Security numbers are now presumed to be public

---

<sup>1</sup> Oversight of the Equifax Data Breach: Answers for Consumers: Hearing before the U.S. House Committee on Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection (Oct. 3, 2017) (Prepared Testimony of Richard F. Smith), <https://democrats-energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony-Smith-DCCP-Hrg-on-Oversight-of-the-Equifax-Data-Breach-Answers-for-Consumers-2017-10-03.pdf> [hereinafter *Smith Testimony*].

<sup>2</sup> *The New Reality of Synthetic ID Fraud*, EQUIFAX INC., [https://www.equifax.com/assets/IFS/syntheticID-fraud\\_wp.pdf](https://www.equifax.com/assets/IFS/syntheticID-fraud_wp.pdf) (last accessed May 30, 2018); Daniel Jean, *The Impact of Synthetic Identity Fraud... By the Numbers*, INSIGHTS BLOG (April 19, 2018), <https://insight.equifax.com/impact-synthetic-identity-fraud/>; Cathleen Donahoo, *How Fraudsters Are Using Synthetic Identities*, INSIGHTS BLOG (March 28, 2018), <https://insight.equifax.com/how-fraudsters-are-using-synthetic-identities/>.



knowledge, and data security experts recommend they never be used again to validate someone's identity. In its simplest terms, Equifax polluted the entire financial services ecosystem by compromising this PII and the ability of financial institutions to verify the identity of any current or potential customer.

10. Plaintiff and the Class have borne, and will continue to bear, the costs associated with Equifax's negligent management of consumer data. When the PII compromised in the Equifax Data Breach was misused, Plaintiff and the Class of financial institutions are required to reimburse consumers for the fraud losses and pay other costs associated with the inability to utilize this data to identify and verify their customers. Plaintiff and the Class also have incurred, and will continue to incur, direct out-of-pocket costs related to this Equifax Data Breach, including to investigating the impact of the Equifax Data Breach, increased monitoring for potentially fraudulent banking activity, reimbursing customers for unauthorized transactions, and communicating with customers regarding their concerns about identity theft and the safety of their financial accounts in light of the Equifax Data Breach. Finally, Plaintiff and the Class face a certainly impending risk of future harm, in the form of future fraudulent banking activity as a direct result of the Equifax Data Breach. This risk of harm will continue into the foreseeable future, have and will require Plaintiff and the Class to incur significant costs and expenses in order to reduce and mitigate this risk of harm.

11. Plaintiff, individually and on behalf of a nationwide class, seeks monetary and non-monetary relief and assert claims against Equifax for negligence (Count 1) and negligence per se (Count 2), as well as for declaratory judgment (Count 3).

#### **PARTIES**

12. Plaintiff First Choice Federal Credit Union is a federally-chartered credit union with a principal place of business in New Castle, Pennsylvania, and is a citizen of Pennsylvania.

As a financial institution that provides financial services, including deposit accounts, credit and/or debit cards, and lending and other credit-related facilities for consumers, Plaintiff First Choice Federal Credit Union is a direct participant in the country's credit reporting system, and both furnishes and receives confidential consumer information (all of which is comprised of and/or is associated with consumers' PII) within that system. In order to provide financial services to consumers, Plaintiff First Choice Federal Credit Union relies on the accuracy and integrity of the information supplied by the credit reporting system, a reliance which is entirely foreseeable by Equifax, given the role that Equifax serves in such system. Plaintiff First Choice Federal Credit Union learned of the Equifax Data Breach when it was publicly announced. In light of the magnitude of the Equifax Data Breach, Plaintiff First Choice Federal Credit Union's current and/or future customers have had their PII compromised, thereby undermining the integrity of the credit reporting system, which has harmed and will continue to harm Plaintiff First Choice Federal Credit Union. Therefore, in response to the public announcement of the Equifax Data Breach, Plaintiff First Choice Federal Credit Union is subject to a greater risk of fraudulent banking activity and has been obligated to investigate the impact of the Equifax Data Breach on the financial institution and its own customers' PII and to implement appropriate additional measures to mitigate the risk of fraudulent banking activity. As a direct result of the Equifax Data Breach, Plaintiff First Choice Federal Credit Union has suffered, and continues to suffer, tangible and intangible harm, including, *inter alia*: (a) direct out of pocket costs related to undertaking an investigation of the impact of the Equifax Data Breach, increased monitoring for potentially fraudulent banking activity, and communicating with customers regarding their concerns about identity theft and the safety of their accounts held at the financial institution in light of the Equifax Data Breach; and (b) a certainly impending risk of future harm, in the form of future fraudulent banking activity, as a direct result

of the compromised PII associated with the Equifax Data Breach, as discussed more fully herein, which will continue into the foreseeable future, and will require Plaintiff First Choice Federal Credit Union to incur significant costs and expenses in order to reduce and mitigate this risk of harm.

13. Defendant Equifax Inc. (“Equifax Inc.”) is a publicly-traded corporation with its principal place of business at 1550 Peachtree Street NE, Atlanta, Georgia. Equifax Inc. represents that it is a leading global provider of information solutions and human resources business process outsourcing services for businesses, governments, and consumers. Equifax further represents that its customers include financial institutions, corporations, governments, and individuals and that it offers products and services based on its comprehensive databases of consumer and business information derived from numerous sources including credit, financial assets, telecommunications and utility payments, employment, income, demographic, and marketing data.

14. Defendant Equifax Information Services LLC (“EIS”) is a wholly-owned subsidiary of Equifax Inc. with its principal place of business at 1550 Peachtree Street NE, Atlanta, Georgia. EIS collects and reports consumer information to financial institutions, including Plaintiff and the Class.

15. Defendants operate together as a consumer reporting agency (“CRA”) to prepare and furnish consumer reports for credit and other purposes.

16. Equifax Inc. and its subsidiaries have eliminated nearly all corporate lines between their formal business entities in the collection, maintenance, sharing, and furnishing of consumer reporting information. Equifax Inc. entities such as EIS regularly and freely share confidential consumer information with sibling entities so all entities, and ultimately Equifax Inc., can market and profit from the sale of information solutions and consumer identity theft protection products.

17. Throughout the events at issue here, Defendants have operated as one entity and CRA. As it pertains to consumer reporting, Equifax Inc. has used EIS as a dependent and integrated division rather than as a separate legal entity. The business operations are fully coordinated and shared. Resources are cross-applied without recognizing full and complete cost and profit centers. Management decisions at EIS are made by and through management of Equifax Inc. The management of Equifax Inc. was and is directly involved in the events at issue in this litigation, including Equifax's cybersecurity, the Data Breach itself, and Defendants' response to the Data Breach.

18. To remain separate and distinct for the purposes of liability in this action, Defendants must operate as separate and distinct legal and operational entities. Here, for the matters and functions alleged and relevant herein, EIS was merely an alter ego of Equifax Inc. For purposes of how consumer data was handled, warehoused, used, and sold, the corporate distinctions were disregarded in practice. EIS was a mere instrumentality for the transaction of the corporate consumer credit business. Defendants shared full unity of interest and ownership such that the separate personalities of the corporation and subsidiary no longer existed. Further, recognition of the technical corporate formalities in this case would cause irreparable injustice and permit Equifax Inc. – the entity whose management caused and permitted the events alleged herein – to defeat justice and to evade responsibility. *See Good v. Holstein*, 787 A.2d 426, 430 (Pa. Super. Ct. 2001); *S.T. Hudson Engineers, Inc. v. Camden Hotel Dev. Assocs.*, 747 A.2d 931 (Pa. Super. Ct. 2000).

19. Accordingly, for all purposes hereafter, when Plaintiff alleges “Equifax” as the actor or responsible party, it is alleging the participation and responsibility of Equifax Inc. and EIS collectively.

## **JURISDICTION AND VENUE**

1. The Court has subject matter jurisdiction over this action pursuant to Pa. Cons. Art. 5, § 5(b) and 42 Pa. C.S.A. § 931(b).

2. The Court has personal jurisdiction over Defendants pursuant to 42 Pa. C.S.A. § 5301(a)(2).

3. Venue is proper in this County pursuant to Pa. R. Civ. P. 2179(a)(2) and (3) because Defendants regularly conducts business in this county and the cause of action arose in this county.

## **FACTUAL ALLEGATIONS**

### **As One of the “Big Three” CRAs, Equifax Is at the Center of the Credit-Based U.S. Economy**

20. Equifax is one of the “big three” CRAs, along with Experian and TransUnion. CRAs, including Equifax, accumulate data relating to consumers from various sources; compile that data in a usable format known as a credit report; and sell access to those reports to lenders interested in making credit decisions as well as financial companies, employers, and other entities that use those reports to make decisions about individuals in a range of areas. Because the extension of credit relies on access to consumers’ credit files, the CRAs have been referred to as the “linchpins” of the U.S. financial system.<sup>3</sup>

21. In a consumer credit system, financial institutions provide the means for consumers to borrow money or incur debt, and to defer repayment of that money over time. The provision of credit by financial institutions enables consumers to buy goods or assets without having to pay for them in cash at the time of purchase.<sup>4</sup> Nearly all Americans rely on credit to make everyday

---

<sup>3</sup> AnnaMaria Andriotis, Michael Rapoport, & Robert McMillan, *‘We’ve Been Breached’: Inside the Equifax Hack*, THE WALL STREET JOURNAL (Sept. 18, 2017), <https://www.wsj.com/articles/weve-been-breached-inside-the-equifax-hack-1505693318>.

<sup>4</sup> M. Greg Braswell and Elizabeth Chernow, *Consumer Credit Law & Practice in the U.S.*, THE U.S. FEDERAL TRADE COMMISSION at 1, <https://www.ftc.gov>



purchases using credit cards, obtain student loans and further education, gain approval for items like cellular phones and Internet access, and to make major life purchases such as automobiles and homes.

22. “The U.S. credit reporting system encompasses a vast flow and store of information.”<sup>5</sup> Indeed, “[c]redit report accuracy relies on an ongoing ecosystem involving the interaction of [CRAs], furnishers of information, public record repositories, users of credit reports, and consumers.”<sup>6</sup>

23. Today, creditors such as credit unions and banks, like Plaintiff and the Class, loan money to consumers, track the consumers’ payment history on the loan, and then provide that information to one or more CRAs. The CRAs track the payment history creditors submit relating to an individual consumer and compile that information into a consumer’s credit reporting “file.”<sup>7</sup>

24. A consumer’s credit file contains identifying information such as the consumer’s name, date of birth, address, and Social Security number, as well as payment information on past credit accounts, including the name of the lender, the original amount of the loan, the type of the loan, and how much money the consumer still owes on the loan. A credit file also contains information in the public record that might affect the consumer’s ability to pay back a loan, such as recent bankruptcy filings, pending lawsuits, or tax liabilities.<sup>8</sup>

---

/sites/default/files/attachments/training-materials/lawpractice.pdf (last accessed May 29, 2018) [hereinafter FTC, *Consumer Credit Law & Practice in the U.S.*].

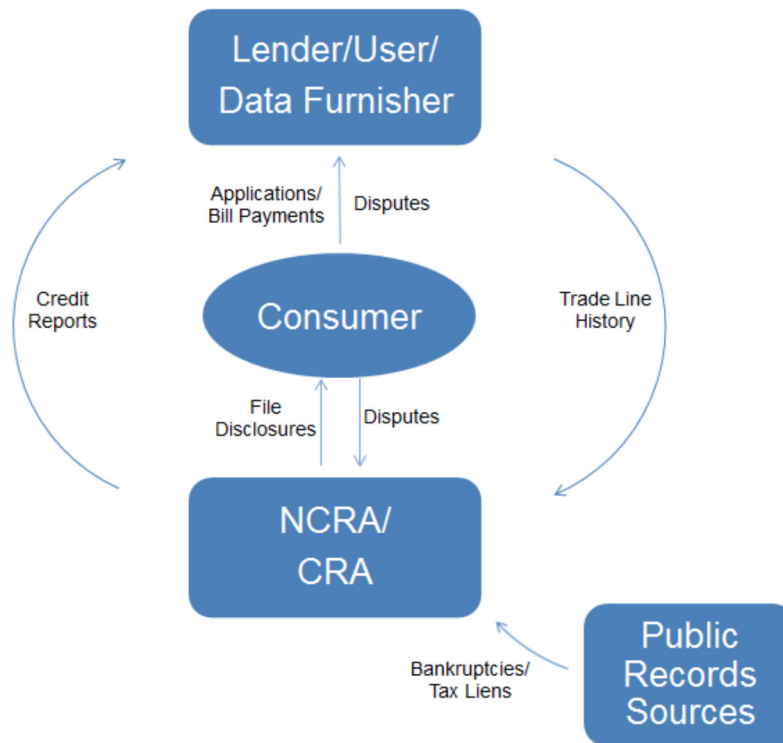
<sup>5</sup> *Key Dimensions and Processes in the U.S. Credit Reporting System*, CONSUMER FINANCIAL PROTECTION BUREAU, at 3 (December 2012), available at [https://files.consumerfinance.gov/f/201212\\_cfpb\\_credit-reporting-white-paper.pdf](https://files.consumerfinance.gov/f/201212_cfpb_credit-reporting-white-paper.pdf).

<sup>6</sup> *Id.* at 6.

<sup>7</sup> FTC, *Consumer Credit Law & Practice in the U.S.*, *supra* n.4 at 1.

<sup>8</sup> *Id.* at 1.

25. The following depicts the flow of data among the participants in the consumer credit system:<sup>9</sup>



26. Financial institutions such as Plaintiff and the Class make up the most significant segment of furnishers of data to the CRAs. According to a study by the Consumer Finance Protection Bureau (“CFPB”), approximately 40% of trade lines in the major CRAs’ files relate to bank payment cards; 18% are from banks that issue retail cards; and the remainder are from collection agencies, debt buyers, the education industry, sales finance lenders, mortgage lenders, auto lenders, or other various creditors.<sup>10</sup>

27. Although the three nationwide CRAs collect information independently and do not have identical data, there is substantial overlap in their databases as a result of the standardization

<sup>9</sup> *Key Dimensions and Processes in the U.S. Credit Reporting System*, CONSUMER FINANCIAL PROTECTION BUREAU, at 13 (Dec. 2012), available at [https://files.consumerfinance.gov/f/201212\\_cfpb\\_credit-reporting-white-paper.pdf](https://files.consumerfinance.gov/f/201212_cfpb_credit-reporting-white-paper.pdf).

<sup>10</sup> *Id.* at 14.

in reporting formats and the tendency of most major furnishers to report their consumer data to multiple CRAs.<sup>11</sup> Even if a particular furnisher or financial institution reports its customers' data to just one CRA, the other CRAs nevertheless can and often do possess much of the same PII for those same customers through consumer data received from other furnishers.<sup>12</sup>

28. Plaintiff and the Class rely on the very PII elements that were exposed in the Equifax Data Breach, not only to determine a consumer's creditworthiness, but also to verify the identity of their customers for all the financial services they offer.

29. Consequently, the size and scope of Equifax's Data Breach has damaged the entire credit and financial services ecosystem. The exposure of such a large amount of PII tied to current and potential customers of Plaintiff and the Class has harmed and will continue to harm them all, including those Plaintiff and Class members that did not furnish their customers' information directly to Equifax.

### **Equifax Compiles Massive Amounts of Consumer Data**

30. Founded in 1899, Equifax is the oldest and second-largest CRA with \$3.1 billion in revenue in 2016.<sup>13</sup> Over 25% of its revenue is generated from the services Equifax offers to its customers in the financial services industry, like Plaintiff and the Class.<sup>14</sup> Equifax represents that it obtains and manages consumer data on over 820 million individuals and over 91 million businesses.<sup>15</sup>

---

<sup>11</sup> *Report to Congress on the Fair Credit Reporting Act Dispute Process*, FEDERAL TRADE COMMISSION AND FEDERAL RESERVE BOARD, at 5 (Aug. 2006), *available at* <https://www.federalreserve.gov/boarddocs/rptcongress/fcradispute/fcradispute200608.pdf>.

<sup>12</sup> This overlap in coverage is especially likely between Equifax and Experian, the largest two CRAs, because each possesses credit information on at least 800 million individuals.

<sup>13</sup> Equifax Inc., Annual Report (Form 10-K) (Feb. 22, 2017) at 27.

<sup>14</sup> *Id.* at 4.

<sup>15</sup> *Id.* at 2.

31. Equifax’s marketing motto is “Powering the World with Knowledge” and it claims to be “a leading global provider of information solutions . . . for businesses, governments and consumers.”<sup>16</sup> To that end, Equifax states that it uses “advanced statistical techniques and proprietary software tools to analyze all available data, creating customized insights, decision-making solutions and processing services for our clients.”<sup>17</sup>

32. According to Equifax, its “products and services are based on comprehensive databases of consumer and business information derived from numerous sources, including credit, financial assets, telecommunications and utility payments, employment, income, demographic and marketing data.”<sup>18</sup> Credit card companies, banks, credit unions, retailers, auto and mortgage lenders all report the details of consumer credit activity to Equifax.<sup>19</sup> In a speech at the University of Georgia, former Equifax CEO Richard Smith explained that Equifax gets its data for free because consumers hand it over to the banks when they apply for credit and that Equifax then crunches the data with the help of computer scientists and artificial intelligence and sells it back to the banks generating a gross margin of about 90 percent.<sup>20</sup>

33. Equifax takes the information that it collects and sells four primary data products: credit services, decision analytics, marketing services, and consumer assistance services.<sup>21</sup> In

---

<sup>16</sup> *Id.*

<sup>17</sup> *Id.*

<sup>18</sup> *Id.*

<sup>19</sup> *How Do Credit Reporting Agencies Get Their Information?* EQUIFAX INC., (July 2, 2014), <https://blog.equifax.com/credit/how-do-credit-reporting-agencies-get-their-information/>.

<sup>20</sup> Michael Riley, Jordan Robertson, and Anita Sharpe, *The Equifax Hack Has the Hallmarks of State-Sponsored Pros*, BLOOMBERG (Sept. 29, 2017 9:09 AM), <https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros>.

<sup>21</sup> Equifax Inc., Annual Report (Form 10-K) (Feb. 22, 2017) at 3.

essence, Equifax's primary business asset is consumer data, which is in part comprised of PII data elements that Equifax algorithmically analyzes and sells to its customers.

**Equifax Knows that Its Consumer Data Must Be Accurate and Adequately Safeguarded**

34. Equifax acknowledges that it is "subject to numerous laws and regulations governing the collection, protection and use of consumer credit and other information, and imposing sanctions for the misuse of such information or unauthorized access to data," including the Fair Credit Reporting Act ("FCRA"), 18 U.S.C. §§1681, *et seq.*, the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§41, *et seq.*, Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. §§6801, *et seq.*, and state unfair and deceptive trade practices acts.<sup>22</sup>

35. Because of the widespread use of credit reports, the accuracy of such reports is an ongoing policy concern, as reflected in the FCRA, 18 U.S.C. §§1681, *et seq.*, which governs the accuracy, fairness and privacy of information in the files of the CRAs. Equifax is subject to the FCRA as a CRA as defined in 15 U.S.C. §§1681a(f) and (p).

36. In the FCRA, Congress emphasized the need to maintain the integrity of the credit reporting system and recognized the dependence of the "banking system" as a whole on the reliability of credit reporting information:

**(a) Accuracy and fairness of credit reporting.**

The Congress makes the following findings:

(1) ***The banking system is dependent upon fair and accurate credit reporting. Inaccurate credit reports directly impair the efficiency of the banking system,*** and unfair credit reporting methods undermine the public confidence which is essential to the continued functioning of the banking system. [Emphasis added].

(2) An elaborate mechanism has been developed for investigating and evaluating the credit worthiness, credit standing, credit capacity, character, and general reputation of consumers.

---

<sup>22</sup> *Id.* at 10.



(3) Consumer reporting agencies have assumed a vital role in assembling and evaluating consumer credit and other information on consumers.

(4) There is a need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy.

15 U.S.C. §1681.

37. The FCRA also recognizes a duty to maintain reasonable procedures in order to protect the confidentiality, accuracy, and proper use of credit information.

(b) Reasonable procedures

It is the purpose of this subchapter to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of this subchapter.

15 U.S.C. §1681.

38. In a 2007 report on credit scores used in lending decisions, the Federal Reserve Board also commented on the importance of accurate credit reports, stating: “for the full benefits of the credit-reporting system to be realized, credit records must be reasonable, complete, and accurate.”<sup>23</sup>

39. The accuracy of credit report information cannot be guaranteed without safeguards to maintain the confidentiality of consumer data. To this end, the GLBA regulates, among other things, the use of non-public personal information of consumers that is held by CRAs and financial institutions. The GLBA's provisions and implementing regulations include rules relating to the

---

<sup>23</sup> *Report to Congress on Credit Scoring and its Effects on the Availability and Affordability of Credit*, FEDERAL RESERVE BOARD (Aug. 2007) (Board Credit Scoring Report), available at <http://www.federalreserve.gov/boarddocs/rptcongress/creditscore/creditscore.pdf>.

use or disclosure of the underlying data and rules relating to the physical, administrative, and technological protection of non-public personal financial information.

40. The Federal Trade Commission (“FTC”) issued the Standards for Safeguarding Customer Information Rule (“Safeguards Rule”), 16 C.F.R. Part 314, implement Section 501(b) of the GLBA, 15 U.S.C. §6801(b).

41. Equifax is subject to the requirements of the Safeguards Rule as a “financial institution,” as that term is defined by Section 509(3)(A) of the GLBA, 15 U.S.C. §6809 (3)(A).

42. Section 501(b) of the GLBA, 15 U.S.C. §6801(b), requires Equifax to follow specific standards regarding the protection of customer information. Specifically, §6801(b) states:

It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.

(b) Financial institutions safeguards

In furtherance of the policy in subsection (a) of this section, each agency or authority described in section 6805(a) of this title shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards –

- 1) to insure the security and confidentiality of customer records and information;
- 2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
- 3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

43. The Safeguards Rule requires Equifax to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards that include: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and

integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§314.3, 314.4.

44. As Equifax well knows, Plaintiff and the Class also are governed by the accuracy and safeguards requirements of these laws. Plaintiff and the Class are participants in the same regulatory regime described above as Equifax. Indeed, information provided by financial institutions to CRAs must be protected at every level. *See, e.g.*, Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. Part 225 App. F, 12 C.F.R. Part 570 App. B, 12 C.F.R. Part 748 App. A, 12 C.F.R. Part 364 App. B, 12 C.F.R. Part 208 App. D-2, 12 C.F.R. Part 30 App. B.

45. Section 5 of the FTC Act, 15 U.S.C. §45, prohibits “unfair . . . practices in or affecting commerce.” The FTC interprets Section 5 the FTC Act to require reasonable data security measures. Many states also have enacted similar statutes that require reasonable data security measures.

46. The foregoing statutes placed a duty on Equifax to act reasonably in managing consumer data and to use reasonable data security measures. In light of the foregoing regulatory regime and the following public statements as well as Equifax's unique position in the credit reporting and financial services ecosystem, Plaintiff and the Class reasonably relied on Equifax to

safeguard consumer data so that such data remained accurate within the credit reporting and financial services ecosystem. Furthermore, as discussed below, Equifax fully intended Plaintiff and the Class to so rely.

**Equifax Represents that Its Consumer Data Is Accurate and Is Adequately Safeguarded**

47. Equifax actively recruits financial institutions, like Plaintiff and the Class, to furnish their consumer data to Equifax, urging: “Reporting your data to Equifax supports the development of comprehensive consumer credit profiles, which benefits both consumers and the greater business community.”<sup>24</sup> Equifax also emphasizes: “Furnishers who report data to Equifax play a vital role in helping identify credit risk and reduce financial losses throughout the entire credit granting community.”<sup>25</sup>

48. Equifax says “Reporting Data is a Win-Win Situation,” and specifically encourages financial institutions to furnish their consumer data to Equifax because it is “Safe, Simple, Secure.”<sup>26</sup> One of the key benefits of furnishing data, according to Equifax, is that the customer can: “Gain more peace of mind by working with a *trusted data provider with industry-leading data security and protection protocols*.”<sup>27</sup> To this end, Equifax explains:

Equifax is a trusted steward of credit information for thousands of financial institutions and businesses, and millions of consumers. *We take this responsibility seriously, and follow a strict commitment to data excellence that helps lenders get the quality information they need to make better business decisions.*

*What’s more, in today’s environment of increasingly complex data privacy and security regulations, we provide businesses with more peace of mind and*

---

<sup>24</sup> *Prospective Data Furnishers Frequently Asked Questions*, EQUIFAX INC., available at [https://assets.equifax.com/assets/usis/data\\_furnisher\\_faq.pdf](https://assets.equifax.com/assets/usis/data_furnisher_faq.pdf) (last accessed May 30, 2018).

<sup>25</sup> *Guidebook for Prospective Data Furnishers*, EQUIFAX INC., available at: [https://assets.equifax.com/assets/usis/data\\_furnisher\\_guidebook.pdf](https://assets.equifax.com/assets/usis/data_furnisher_guidebook.pdf) (last accessed May 30, 2018).

<sup>26</sup> *Consumer Data Reporting*, EQUIFAX INC., available at [https://assets.equifax.com/assets/usis/dataFurnishersConsumerCreditData\\_ps.pdf](https://assets.equifax.com/assets/usis/dataFurnishersConsumerCreditData_ps.pdf) (last accessed May 30, 2018).

<sup>27</sup> *Id.*

*confidence when it comes to data reporting, and expert security compliance teams who are dedicated to data protection.*<sup>28</sup> [Emphasis added].

49. Equifax readily acknowledges the importance of consumer data furnished by financial institutions such as Plaintiff and the Class, stating that the loss of such data is a risk factor to its business: “We rely extensively upon data from external sources to maintain our proprietary and non-proprietary databases, including data received from customers, strategic partners and various government and public record sources. This data includes the widespread and voluntary contribution of credit data from most lenders in the U.S.”<sup>29</sup>

50. In its 2016 Form 10-K, Equifax touted itself as a “trusted steward and advocate for our customers and consumers” and stated that it was “continuously improving the customer and consumer experience in our consumer and commercial offerings, anticipating and executing on regulatory initiatives, while simultaneously delivering security for our services.”<sup>30</sup> It also claimed: “Data is at the core of our value proposition.”<sup>31</sup>

51. As to its regulatory obligations, Equifax acknowledged that it is “subject to numerous laws and regulations governing the collection, protection and use of consumer credit and other information, and imposing sanctions for the misuse of such information or unauthorized access to data,” including the FCRA, FTC Act, GLBA, and state unfair and deceptive trade practices actions.<sup>32</sup>

52. Specifically, Equifax acknowledged that the “security measures we employ to safeguard the personal data of consumers could also be subject to the FTC Act.”<sup>33</sup> It also admitted

---

<sup>28</sup>

*Id.*

<sup>29</sup>

Equifax Inc., Annual Report (Form 10-K) (Feb. 22, 2017) at 15.

<sup>30</sup>

*Id.* at 4.

<sup>31</sup>

*Id.* at 3.

<sup>32</sup>

*Id.* at 10.

<sup>33</sup>

*Id.*



that it must comply with the FCRA, which governs the accuracy, fairness, and privacy of information in the credit files Equifax maintains, as well as the GLBA's "rules relating to the physical, administrative and technological protection of non-public personal financial information."<sup>34</sup> Similarly, Equifax recognized that data furnishers and users of credit information, like Plaintiff and the Class, are subject to these same regulations.<sup>35</sup> Equifax also conceded that numerous state data security breach laws "require additional data protection measures which exceed the GLBA data safeguarding requirements," and that "[i]f data within our system is compromised by a breach, we may be subject to provisions of various state security breach laws."<sup>36</sup>

53. Equifax claimed that it devoted "substantial compliance, legal and operational business resources to facilitate compliance with applicable regulations and requirements,"<sup>37</sup> and that it had made a "substantial investment in physical and technological security measures."<sup>38</sup>

54. In its privacy statements, Equifax echoed these promises that it would provide accurate data and that it would adequately safeguard this data. Equifax's summary statement of its privacy policy on its website specifically states: "We have built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. . . . Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax."<sup>39</sup> Equifax's privacy policy further states: "We are committed to protecting the security of your personal information and use technical, administrative and physical security measures that

---

<sup>34</sup>

*Id.*

<sup>35</sup>

*Id.*

<sup>36</sup>

*Id.* at 11.

<sup>37</sup>

*Id.* at 18.

<sup>38</sup>

*Id.* at 16.

<sup>39</sup>

*Privacy*, EQUIFAX INC., <https://www.equifax.com/privacy/> (last accessed May 30, 2018).

*comply with applicable federal and state laws,”*<sup>40</sup> and that “[w]e have reasonable physical, technical and procedural safeguards to help protect your personal information.”<sup>41</sup> [Emphasis added].

55. On another privacy policy webpage, Equifax similarly emphasized that it would “take reasonable steps to . . . [u]se safe and secure systems, including physical, administrative, and technical security procedures to safeguard the information about you.” It promoted that it had

security protocols and measures in place to protect the personally identifiable information . . . and other information [it] maintain[ed] about you from unauthorized access or alteration. These measures include internal and external firewalls, physical security and technological security measures, and encryption of certain data. When personally identifiable information is disposed of, it is disposed of in a secure manner.<sup>42</sup>

56. In its 2016 Form 10-K, Equifax acknowledged not only its obligation to protect the consumer data it obtains, stores, uses, transmits, sells, and manages, but also the risk that a data breach could occur at Equifax and the impact such a breach would have on Equifax, consumers, and customers:

***[W]e collect and store sensitive data, including intellectual property, proprietary business information and personally identifiable information of our customers, employees, consumers and suppliers, in data centers and on information technology networks. The secure and uninterrupted operation of these networks and systems, and of the processing and maintenance of this information, is critical to our business operations and strategy.***

Despite our substantial investment in physical and technological security measures, employee training, contractual precautions and business continuity plans, our information technology networks and infrastructure or those of our third-party vendors and other service providers could be vulnerable to damage, disruptions, shutdowns, or breaches of confidential information due to criminal conduct, denial

---

<sup>40</sup> *Equifax Personal Products*, EQUIFAX INC., <https://www.equifax.com/privacy/equifax-personal-products/#EffortsWeMakeToSafeguardYourPersonalInformation> (last accessed May 30, 2018).

<sup>41</sup> *Personal Credit Reports*, EQUIFAX INC., <https://www.equifax.com/privacy/personal-credit-reports/> (last accessed May 30, 2018).

<sup>42</sup> *Privacy Policy*, EQUIFAX INC., [https://www.equifax.com/cs/Satellite?pagename=privacy\\_optout](https://www.equifax.com/cs/Satellite?pagename=privacy_optout) (last accessed May 30, 2018).

of service or other advanced persistent attacks by hackers, employee or insider error or malfeasance, or other disruptions during the process of upgrading or replacing computer software or hardware, power outages, computer viruses, telecommunication or utility failures or natural disasters or other catastrophic events. ***Unauthorized access to data files or our information technology systems and applications could result in inappropriate use, change or disclosure of sensitive and/or personal data of our customers, employees, consumers and suppliers.***

***We are regularly the target of attempted cyber and other security threats and must continuously monitor and develop our information technology networks and infrastructure to prevent, detect, address and mitigate the risk of unauthorized access, misuse, computer viruses and other events that could have a security impact. Insider or employee cyber and security threats are increasingly a concern for all large companies, including ours. Although we are not aware of any material breach of our data, properties, networks or systems, if one or more of such events occur, this potentially could compromise our networks and the information stored there could be accessed, publicly disclosed, lost or stolen. Any such access, disclosure or other loss of information could subject us to litigation, regulatory fines, penalties or reputational damage, any of which could have a material effect on our cash flows, competitive position, financial condition or results of operations.***<sup>43</sup> [Emphasis added].

57. In light of the foregoing statements, Equifax intended Plaintiff and the Class to rely on Equifax to provide accurate data and to adequately safeguard that data. Plaintiff reasonably expected that such information would be stored by Equifax in a safe and confidential manner, using all reasonable safeguards and protections. The potential harm from doing otherwise was obvious to Equifax, which knew that Plaintiff and the Class, as payment card issuers, lenders, and deposit account holders, would bear the ultimate responsibility for identity theft and fraudulent lending and other consumer transactions that would occur if the consumer data were compromised.

58. Equifax explicitly recognized Plaintiff's reliance on the information it provides, stating: "[o]ur products and services enable businesses to make credit and service decisions, manage their portfolio risk, automate or outsource certain payroll-related, tax and human resources businesses processes, and develop certain marketing strategies concerning consumers and

---

<sup>43</sup> Equifax Inc., Annual Report (Form 10-K) (Feb. 22, 2017) at 17.

commercial enterprises.”<sup>44</sup> Equifax also stated: “Businesses rely on us for consumer and business credit intelligence, credit portfolio management, fraud detection, decisioning technology, marketing tools, debit management and human resources-related services.”<sup>45</sup>

59. Much like a bailment of personal property, the receipt by Equifax of uniquely-identifying consumer credit-reporting information, PII,— for Equifax’s own business purposes — places Equifax in a special relationship with Plaintiff and the Class, which rely on Equifax to maintain the security (and hence, the uniquely-identifying nature) of such information. The resulting harm to Plaintiff and the Class from mishandling the security and confidentiality of the credit information was, at all times, foreseeable to Equifax.

**Equifax Knew that a Breach of Its Computer Systems Was a Foreseeable Risk**

60. With data breaches and identity theft on the rise, Equifax undoubtedly knew that a breach of its computer systems was a foreseeable risk. It also knew what the repercussions of such a breach would be.

61. PII and Payment Card Data have considerable value and constitute an enticing and well-known target to hackers. Hackers easily can sell such stolen data as a result of the “proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce.”<sup>46</sup>

62. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. According to the Identity Theft Resource Center (“ITRC”),

---

<sup>44</sup> *Id.* at 60.

<sup>45</sup> *Id.* at 29.

<sup>46</sup> Brian Krebs, *The Value of a Hacked Company*, KREBS ON SECURITY (July 14, 2016, 10:47 AM), <http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/>.

in 2017 there were 1,579 reported data breaches in the United States, an all-time high.<sup>47</sup> More than 178.93 million records reportedly were exposed in those breaches (approximately 147.9 million of which were exposed in the Equifax Data Breach alone).<sup>48</sup> The IRTC reported that approximately 60% of the data breaches were the result of hacking.<sup>49</sup>

63. In tandem with the increase in data breaches, the rate of identity theft also reached record levels in 2017, affecting approximately 16.7 million victims in the U.S., with the amount stolen rising to \$16.8 billion.<sup>50</sup>

64. Following several high-profile data breaches in recent years, including those involving Target, Experian, Yahoo, Home Depot, and Sony, Equifax was on notice of the very real risk that hackers could exploit vulnerabilities in its data security.

65. These and other data breaches have been well publicized. Unfortunately, Equifax did not view these breaches as cautionary tales, but rather as another avenue to profit from businesses and consumers concerned with fraud. Equifax's CEO Richard Smith admitted as much in an August 2017 speech where he referred to consumer fraud as a "huge opportunity" and "massive, growing business" for Equifax.<sup>51</sup>

### **Equifax Knew What the Repercussions of a Data Breach Would Be**

---

<sup>47</sup> *Data Breach Reports: 2017 End of Year Report*, IDENTITY THEFT RESOURCE CENTER, at 6 (2018), [http://www.idtheftcenter.org/images/breach/2017/DataBreachReport\\_2017.pdf](http://www.idtheftcenter.org/images/breach/2017/DataBreachReport_2017.pdf).

<sup>48</sup> *Id.*

<sup>49</sup> *Id.* at 4.

<sup>50</sup> Press Release, Javelin Strategy & Research, *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study* (Feb. 6, 2018), <https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin>.

<sup>51</sup> Jim Puzzanghera, *Senators Slam Equifax for making money off massive data breach and no-bid IRS contract*, LOS ANGELES TIMES (Oct. 4, 2017), <http://www.latimes.com/business/la-fi-equifax-senate-20171004-story.html>; Megan Leonhardt, *Equifax Is Going to Make Millions Off Its Own Data Breach*, TIME (Oct. 4, 2017), <http://time.com/money/4969163/equifax-hearing-elizabeth-warren-richard-smith/>.



66. As evidenced by its own product offerings, Equifax held itself out as a leader and expert in anticipating and combatting cybersecurity threats. In marketing these solutions, data security was Equifax's sales pitch.<sup>52</sup>

67. Equifax even developed and sold "data breach solutions" to financial institutions, like Plaintiff and the Class, to combat the "great risk of identity theft and fraud." Equifax maintains a dedicated landing page to sell products and services: <https://www.equifax.com/help/data-breach-solutions>.



68. In its marketing materials, Equifax states: "You'll feel safer with Equifax. We're the leading provider of data breach services, serving more than 500 organizations with security breach events every day. In addition to extensive experience, Equifax has the most comprehensive set of identity theft products and customer service coverage in the market."<sup>53</sup>

### **Data Breaches are on the rise. Be prepared.**

You'll feel safer with Equifax. We're the leading provider of data breach services, serving more than 500 organizations with security breach events everyday. In addition to extensive experience, Equifax has the most comprehensive set of identity theft products and customer service coverage in the market.

<sup>52</sup> Stacy Cowley & Tara Siegel Bernard, *As Equifax Amassed Ever More Data, Safety Was a Sales Pitch*, NEW YORK TIMES (Sept. 23, 2017), <https://www.nytimes.com/2017/09/23/business/equifax-data-breach.html>.

<sup>53</sup> *Equifax Data Breach Solutions*, EQUIFAX INC., <https://www.equifax.com/help/data-breach-solutions> (last accessed May 30, 2018).

69. Equifax also has touted its “Data Breach Response Team,” which includes a “dedicated group of professionals that will implement a ‘data breach response plan’ before a breach ever occurs,” including informing “consumers, employees, and shareholders with pre-defined communications” regarding the breach, offering identity theft protection products, providing a dedicated call center to assist breach victims, and placing fraud alerts on consumers’ credit files.<sup>54</sup>

### **Experienced help is here.**

Equifax can help you prepare with our Equifax Data Breach Response Team — a dedicated group of professionals that will implement a “data breach response plan” before a breach ever occurs.

### **Here's how our Response Team provides peace of mind.**

We consult with you to create a customized Data Breach Response Plan that will enable you to:

- 1 Quickly inform consumers, employees, and shareholders with pre-defined communications regarding the event and the steps you are taking on their behalf ;
- 2 Offer the appropriate level of identity theft protection products based on the risk profile of the data breach (ask about our Data Breach Risk Assessment Matrix);
- 3 Provide a dedicated Call Center to assist breached victims with product related questions after enrollment.
- 4 Place Fraud Alerts on consumers' credit files at all three credit reporting agencies as requested.

70. Equifax even summarized some of the repercussions of a data breach, including the erosion of employee and customer trust, decline in shareholder value, undesirable publicity, legal and regulatory liabilities, and out of budget expenses. Equifax, therefore, fully understood the consequences of failing to secure its data.<sup>55</sup>

### **Consider what a breach can do.**

Knowing that a data breach is a very real possibility, your company needs to be prepared for it.

After all, a breach can have many serious implications:

- Erosion of employee customer trust
- Decline in shareholder value
- Undesirable publicity
- Legal & regulatory liabilities
- Out of budget expenses

---

<sup>54</sup> *Id.*

<sup>55</sup> *Id.*

71. In 2017, Equifax’s Chief Information Security Officer (“CISO”), Susan Mauldin, was interviewed about “how the role of a Chief Information Security Officer has evolved in response to growing cybersecurity threats.”<sup>56</sup> In the interview, Ms. Mauldin discussed at length her methods for addressing expected cybersecurity threats, stating: “We spend our time looking for threats against a company. We look for things that might be active inside the company that would cause us concern, and then of course we look to respond – detecting, containing and deflecting those threats.”<sup>57</sup> She went on to outline some of her “best practices” for combatting cybersecurity threats. It was later revealed that Ms. Mauldin had no formal training in information systems or cybersecurity; rather, her training was in music composition.

72. Thus, Equifax knew, given the vast amount of PII it managed, that it was a “regular” target of attempted cyber and other security threats and therefore understood the risks posed by its insecure and vulnerable computer systems and website. It also understood the need to safeguard PII and the impact a data breach would have on financial institutions, including Plaintiff and the Class.

### **Equifax Knew that Its Data Security Practices Were Inadequate**

73. Equifax has a long history of maintaining data security measures that are inadequate for the scale and complexity of its business and the sensitivity of the consumer data that it obtains, stores, uses, transmits, sells, and manages. In the months leading up to the Data Breach, Equifax experienced multiple security breaches, where consumer PII was compromised as a result of deficient data security measures. Therefore, Equifax knew that its data security practices were inadequate.

---

<sup>56</sup> Prat Moghe, *Interview with Equifax CISO Susan Mauldin*, CAZENA, <https://web.archive.org/web/20170908175854/https://www.cazena.com/susan-mauldin-transcript> (last visited May 29, 2018).

<sup>57</sup> *Id.*

74. For instance, in March 2015, Equifax admitted “that it mistakenly exposed consumer data as a result of a technical error that occurred during a software change.”<sup>58</sup> Equifax inadvertently mailed credit report information, including Social Security numbers and sensitive account information, to unauthorized individuals who did not request the information.<sup>59</sup> A woman in Maine received from Equifax hundreds of credit reports belonging to others.<sup>60</sup> Equifax later informed the Maine Bureau of Consumer Credit Protection that a software upgrade error led to the mailing of the credit reports to the wrong individuals.<sup>61</sup>

75. In April 2016, Equifax’s W-2Express website (<http://w2express.com>), which allowed employees to access copies of their W-2 tax forms, suffered a data breach in which hackers accessed the salary and tax information of more than 800 current and former employees of Stanford University and Northwestern University through the W-2Express website.<sup>62</sup>

---

<sup>58</sup> Office of Sen. Elizabeth Warren, *Bad Credit: Uncovering Equifax’s Failure to Protect American’s Personal Information* 4 (Feb. 2018), available at [https://www.warren.senate.gov/files/documents/2018\\_2\\_7\\_%20Equifax\\_Report.pdf](https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf) [hereinafter Warren Report]; see also *Emails Reveal New Details About Equifax Data Breach, AG Announces Settlement*, CBS 13 & BANGOR DAILY NEWS (May 30, 2015), available at <https://bangordailynews.com/2015/05/30/news/state/emails-reveal-new-details-about-equifax-data-breach-ag-announces-settlement/> [hereinafter CBS 13 & BANGOR DAILY NEWS, *Emails Reveal New Details*].

<sup>59</sup> *Equifax Discloses Data Breach Due to Technical Error During Software Change*, DATABREACHES.NET (April 9, 2015), <https://www.databreaches.net/equifax-discloses-data-breach-due-to-technical-error-during-software-change/>.

<sup>60</sup> John Chrisos, *Credit Agency Mistakenly Sends 300 Confidential Reports to Maine Woman*, CBS 13 & BANGOR DAILY NEWS (March 19, 2015), <http://bangordailynews.com/2015/03/19/news/state/credit-agency-mistakenly-sends-300-confidential-reports-to-maine-woman/>.

<sup>61</sup> CBS 13 & Bangor Daily News, *Emails Reveal New Details*, *supra* n.58.

<sup>62</sup> Hannah Knowles, *University Employees Vulnerable After Tax Data Breach*, STANFORD DAILY (April 12, 2016), <https://www.stanforddaily.com/2016/04/12/university-employees-vulnerable-after-tax-data-breach/>; see also *Northwestern University Announcement, Update on IRS Tax Filings and W-2 Access*, NORTHWESTERN UNIVERSITY (April 22, 2016), <https://news.northwestern.edu/stories/2016/04/update-on-irs-tax-filings-and-w-2-access/>; Peter Kotecki, *Tax Fraud, Identity Theft Affect More Than 250 Northwestern Employees*, DAILY NORTHWESTERN (April 27, 2016), <https://dailynorthwestern.com/2016/04/27/campus/tax-fraud->

76. Similarly, in May 2016, Equifax's W-2Express website was breached again, resulting in the disclosure of 430,000 names, addresses, Social Security numbers, and other personal information of current and past employees of grocery retail giant Kroger.<sup>63</sup> The W-2Express website breach occurred because Equifax used weak default login information based on users' partial Social Security number and year of birth, information easily obtained by third parties.<sup>64</sup>

77. Then, between April 2016 and March 2017, TALX Corp., an Equifax subsidiary now referred to as Equifax Workforce Solutions that provides online payroll, HR, and tax services, suffered a data breach where hackers stole Equifax customers' employees' W-2 tax data by resetting the employees' 4-digit PIN password after answering personal identifying questions about those employees.<sup>65</sup>

78. In January 2017, a LifeLock customer was able to view several unrelated persons' credit reports through the LifeLock online portal. Equifax researched the issue and acknowledged

---

identity-theft-affect-more-than-250-northwestern-employees/; Lisa M. Krieger, *Some Stanford Employees Are Victims of Social Security Fraud*, MERCURY NEWS (Aug. 25, 2017), <https://www.mercurynews.com/2017/08/25/stanford-victims-of-social-security-fraud/>.

<sup>63</sup> Warren Report, *supra* n.58; see also Thomas Fox-Brewster, *A Brief History of Equifax Security Fails*, FORBES (Sept. 8, 2017), <https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#2661e102677c>; Brian Krebs, *Crooks Grab W-2s from Credit Bureau Equifax*, KREBS ON SECURITY (May 6, 2016), <https://krebsonsecurity.com/2016/05/crooks-grab-w-2s-from-credit-bureau-equifax>.

<sup>64</sup> Jeremy Henley, *The Kroger/Equifax W-2 Breach: What Can We Learn From It*, IDEXPERTS.COM (June 7, 2016), <https://www2.idexperts.com/knowledge-center/single/the-kroger-equifax-w-2-breach-what-can-we-learn-from-it>.

<sup>65</sup> Brian Krebs, *Fraudsters Exploited Lax Security at Equifax's TALX Payroll Division*, KREBS ON SECURITY (May 18, 2017), <https://krebsonsecurity.com/2017/05/fraudsters-exploited-lax-security-at-equifaxs-talx-payroll-division/>.

that credit information of a “small number of LifeLock members” was inadvertently sent to another member’s online portal “as the result of a technical issue.”<sup>66</sup>

79. In light of the foregoing breaches of Equifax’s systems, Equifax knew that its data security practices were inadequate. Equifax also knew or should have known of its many security deficiencies from the criticisms levied by multiple third parties that concluded Equifax was highly susceptible to a data breach.

80. In August 2016, MSCI, Inc. (“MSCI”), an institutional investor research analyst, criticized “Equifax Inc.’s poor data security and privacy measures” and downgraded Equifax to “CCC,” MSCI’s lowest possible rating.<sup>67</sup>

81. In December 2016, MSCI issued a follow-up research report and stated: “Equifax is vulnerable to data theft and security breaches, as is evident from the 2016 breach of 431,000 employees’ salary and tax data of one of its largest customers, Kroger grocery chain. The company’s data and privacy policies are limited in scope and Equifax shows no evidence of data breach plans or regular audits of its information security policies and systems.”<sup>68</sup>

82. Also in December 2016, a security researcher warned Equifax that one of Equifax’s public-facing websites “displayed several search fields, and anyone – with no authentication whatsoever – could force the site to display the personal data of Equifax’s customers.”<sup>69</sup> The flaw

---

<sup>66</sup> Letter from King & Spalding LLP to Attorney General Joseph Foster Regarding Data Incident Notification (Feb. 8, 2017), <https://www.doj.nh.gov/consumer/security-breaches/documents/equifax-20170208.pdf>.

<sup>67</sup> *MSCI ESG Ratings May Help Identify Warning Signs*, MSCI, at 1, <https://www.msci.com/documents/1296102/6174917/MSCI-ESG-Ratings-Equifax.pdf/b95045f2-5470-bd51-8844-717dab9808b9> (last visited May 30, 2018).

<sup>68</sup> *Id.*

<sup>69</sup> Lorenzo Franceschi-Bicchierai, *Equifax Was Warned*, VICE (Oct. 26, 2017), [https://motherboard.vice.com/en\\_us/article/ne3bv7/equifax-breach-social-security-numbers-researcher-warning](https://motherboard.vice.com/en_us/article/ne3bv7/equifax-breach-social-security-numbers-researcher-warning).



was discovered on a webpage that appeared to be a portal for Equifax employees, but was open to anyone on the internet.<sup>70</sup> The researcher accessed full names, Social Security numbers, birth dates, and city and state of residence information for “every American” through Equifax’s unsecured website.<sup>71</sup> The researcher also took control of several Equifax servers and found that the servers were running outdated software vulnerable to further breaches. The researcher immediately reported the security flaw to Equifax and stated: “[i]t should've been fixed the moment it was found. It would have taken them five minutes, they could've just taken the site down.”<sup>72</sup> Instead, it took Equifax six months to patch that vulnerability.<sup>73</sup>

83. In addition, four independent analyses of Equifax’s systems and controls relating to cybersecurity – conducted either before or immediately after the Data Breach – identified serious weaknesses, including that Equifax “was behind on basic maintenance of websites that could have been involved in transmitting sensitive consumer information and scored poorly in areas” highly susceptible to data breaches.<sup>74</sup>

84. In April 2017 – the month before the Data Breach – Cyence, a cyber-risk analysis firm, “rated the danger of a data breach at Equifax during the next 12 months at 50%. It also found the company performed poorly when compared with other financial-services companies.”<sup>75</sup>

---

<sup>70</sup> *Id.*

<sup>71</sup> *Id.*

<sup>72</sup> *Id.*

<sup>73</sup> *Id.*; see also George Cox, *Equifax Suffers Another Security Breach*, THE SPECTRUM (Nov. 8, 2017), <https://www.thespectrum.com/story/life/features/mesquite/2017/11/08/equifaxsuffers-another-security-breach/842717001/>.

<sup>74</sup> AnnaMaria Andriotis & Robert McMillan, *Equifax Security Showed Signs of Trouble Months Before Hack*, THE WALL STREET JOURNAL (Sept. 26, 2017), <https://www.wsj.com/articles/equifax-security-showed-signs-of-trouble-months-before-hack-1506437947>.

<sup>75</sup> Warren Report, *supra* n.58, at 5.



85. SecurityScorecard, another security monitoring firm, identified the precise weakness that was used by the hackers to breach the Equifax system, reporting that “Equifax used older software – such as the Apache Struts tool kit . . . and often seemed slow to install patches.”<sup>76</sup>

86. An outside review by Fair Isaac Corporation (“FICO”) rated Equifax’s “enterprise security score” based on three elements: hardware, network security, and web services. The score declined from 550 out of 800 at the beginning of 2017 to 475 in mid-July 2017. The FICO analysis found that public-facing websites run by Equifax used expired security certificates and had errors in the chain of certificates and other web-security issues. Updated security certificates are vital to data security because they are used to authenticate the connection between a user’s web browser and an HTTPS web server, allowing the user to know that its connection to a website is legitimate and secure.<sup>77</sup>

87. A fourth independent review – released just after the Equifax Data Breach was announced – also identified significant problems with Equifax cybersecurity. This BitSight Technologies report gave Equifax an “F” in application security and a “D” for software patching.<sup>78</sup>

88. These criticisms underscored Equifax’s own awareness that it was highly susceptible to a data breach.

#### **Equifax Ignored the Notification of the Specific Vulnerability That Led to the Data Breach**

89. On September 7, 2017, Equifax announced that between May 13, 2017 and July 30, 2017, hackers exploited a vulnerability in Equifax’s U.S. web server software to gain access to the PII of approximately 143 million U.S. consumers and the Payment Card Data of 209,000

---

<sup>76</sup> *Id.*

<sup>77</sup> *Id.*

<sup>78</sup> *Id.*

cardholders.<sup>79</sup> The estimated number of U.S. consumers impacted by the Data Breach later was increased to 147.9 million.<sup>80</sup>

90. The attack vector used in this incident occurred through vulnerabilities in Apache Struts (CVE-2017-5638), an open-source application framework that supports the Equifax online dispute portal web application.<sup>81</sup>

91. Equifax's online dispute portal, which is located at <https://www.equifax.com/personal/disputes/>, allows consumers to dispute inaccurate information contained on their credit files.

92. To access the online dispute portal, a user must input certain PII, including name, address, Social Security number, date of birth, and email address, along with an optional ten digit confirmation code, which is the confirmation number found on the copy of a customer's credit file, or the confirmation number provided by Equifax when the customer created the online dispute.

---

<sup>79</sup> *Equifax Announces Cybersecurity Incident Involving Consumer Information*, EQUIFAX INC., (Sept. 7, 2017), <https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628>.

<sup>80</sup> AnnaMaria Andriotis, *Equifax Identifies Additional 2.4 Million Affected by 2017 Breach*, THE WALL STREET JOURNAL (March 1, 2018), <https://www.wsj.com/articles/equifax-identifies-additional-2-4-million-affected-by-2017-breach-1519918282>.

<sup>81</sup> *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, EQUIFAX INC., (Sept. 15, 2017), <https://www.equifaxsecurity2017.com/2017/09/15/equifax-releases-details-cybersecurity-incident-announces-personnel-changes/>.

**EQUIFAX®** Online Dispute

Step 1 Authentication Step 2 Dispute Information Step 3 Upload Documents Step 4 Review & Submit Step 5 Get Confirmation

### Let's locate your credit file

Before you can get started, we'll need to find your Equifax Credit File. To help us locate your file, you will need to provide the following information:

*\*Indicates a mandatory field*

10-Digit Confirmation Number  [What is this?](#)

\*First Name

\*Last Name

Initial  Suffix

\*Social Security Number  -  -

\*Date of Birth  /  /

\*Current Address

\*City

\*State

\*Zip Code

Have you lived at your current address for more than 2 years? ☒ Yes ☐ No

\*Email

\*Confirmation Email

☐ [Show only last 4 digits of my SSN](#)

\* ☐ To continue, click to agree to [Online Delivery of Results](#)

**Continue**

It is the 10-digit confirmation number found on the copy of your Equifax Credit File, or the 10-digit confirmation number provided to you when you created your dispute online.

93. Once a user provides the requested PII, they are able to review information regarding their credit, including their personal information (such as name, address, Social Security number, date of birth), credit history for their accounts (for credit products such as mortgages, loans, and credit cards), amounts owed for each credit product, and any negative information regarding their credit (late payments, collection information, and bankruptcy filings).

**EQUIFAX®** Online Dispute

Step 1 Authentication Step 2 Dispute Information Step 3 Upload Documents Step 4 Review & Submit Step 5 Get Confirmation

Welcome

Please select the area of your credit file you prefer to review. This is a current copy of your file and has the latest information available. Please review carefully.

Equifax allows you to upload image documents in support of your dispute. The allowable formats are JPG, JPEG, TIFF, TIF, PNG, GIF and PDF. If you will be submitting documents with us online, please prepare these documents now before continuing with the dispute options. Multiple documents may be uploaded but each is limited to 3 MB. Please note, when you upload documents, including a letter, to Equifax as part of your dispute, the documents may be submitted to one or more companies whose information are the subject of your dispute. Click [here](#) for more information and image guidelines.

What do you want to dispute? (Select a section below.)

 <b>Personal Information</b> Personal information is any information that may identify you and includes name, address, social security number, date of birth, etc.	 <b>Accounts</b> Account information includes mortgages, home equity loans, installment loans, credit cards and charge cards that are currently paid as agreed.	 <b>Negative Information</b> An account that has not been paid as agreed and may include collections, bankruptcies, liens, and judgments.	 <b>Inquiries</b> A request for your credit history is called an inquiry and is made by companies with whom you have applied or established credit. Inquiries remain on your credit file up to two years.
--	---	---	---

94. As the following images show, all the data contained in the credit file is available once the dispute resolution portal is accessed:

Step 1 Authentication Step 2 Dispute Information Step 3 Upload Documents Step 4 Review & Submit Step 5 Get Confirmation

**Equifax Credit File™ for:** [REDACTED]  
**As of Date:** 05/21/2018

**Personal Information** **Accounts** **Negative Information** **Inquiries**

**Mortgage** **Installments** **Revolving** **Other**

**Mortgage Accounts** **Hide All Account Details** **Show All Account Details** **Show All Dispute Options**  
Includes mortgages, home equity loans, and any other loans secured by real estate.

**Open Accounts**

Name: [REDACTED] Acct #: XXXX Credit Limit: n/a Date Reported: 04/30/2018  
Date Opened: [REDACTED] Balance: [REDACTED] Past Due: \$0 Acct Status: PAYS AS AGREED

**Hide Details** **Dispute Item**

[REDACTED]

Account Number:	XXXX	Current Status:	PAYS AS AGREED
Account Owner:	Joint Account	High Credit:	[REDACTED]
Type of Account ? :	Mortgage	Credit Limit:	N/A
Terms Duration:	[REDACTED]	Terms Frequency:	Monthly (due every month)
Date Opened:	[REDACTED]	Balance:	[REDACTED]
Date Reported:	[REDACTED]	Amount Past Due:	\$0
Date of Last Payment:	[REDACTED]	Actual Payment Amount:	[REDACTED]
Scheduled Payment Amount:	[REDACTED]	Date of Last Activity:	[REDACTED]
Date Major Delinquency First Reported:		Months Reviewed:	12
Creditor Classification:		Activity Description:	N/A
Charge Off Amount:	\$0	Deferred Payment Start Date:	
Balloon Payment Amount:	\$0	Balloon Payment Date:	
Date Closed:		Type of Loan:	yes
Date of First Delinquency:	N/A		
Comments:	[REDACTED]		

**81-Month Payment History**

Year	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
2018	*	*	*									
2017	*	*	*	*	*	*	*	*	*	*	*	*
2016	*	*	*	*	*	*	*	*	*	*	*	*
2015	*	*	*	*	*	*	*	*	*	*	*	*
2014	*	*	*	*	*	*	*	*	*	*	*	*
2013						*	*	*	*	*	*	*

**Mortgage** **Installments** **Revolving** **Other**

**Revolving Accounts** [Show All Account Details](#) [Show All Dispute Options](#)

Accounts that have a credit limit and require a minimum payment each month, such as most credit cards.

**Open Accounts**

Name: [REDACTED] Date Opened: 11/14/1995	Acct #: [REDACTED] Balance: \$ [REDACTED]	Credit Limit: \$ [REDACTED] Past Due: \$0	Date Reported: 05/13/2018 Acct Status: PAYS AS AGREED
<a href="#">Show Details</a>	<a href="#">Dispute Item</a>		
Name: [REDACTED] Date Opened: 12/07/1995	Acct #: [REDACTED] Balance: \$ [REDACTED]	Credit Limit: \$ [REDACTED] Past Due: \$0	Date Reported: 04/23/2018 Acct Status: PAYS AS AGREED
<a href="#">Show Details</a>	<a href="#">Dispute Item</a>		
Name: [REDACTED] Date Opened: 12/11/2005	Acct #: [REDACTED] Balance: \$ [REDACTED]	Credit Limit: \$ [REDACTED] Past Due: \$0	Date Reported: 02/01/2018 Acct Status: PAYS AS AGREED
<a href="#">Show Details</a>	<a href="#">Dispute Item</a>		
Name: [REDACTED] Date Opened: 10/05/2000	Acct #: [REDACTED] Balance: \$0	Credit Limit: \$ [REDACTED] Past Due: \$0	Date Reported: 05/05/2018 Acct Status: PAYS AS AGREED
<a href="#">Show Details</a>	<a href="#">Dispute Item</a>		
Name: [REDACTED] Date Opened: 04/22/2017	Acct #: [REDACTED] Balance: \$0	Credit Limit: \$ [REDACTED] Past Due: \$0	Date Reported: 04/21/2018 Acct Status: PAYS AS AGREED
<a href="#">Show Details</a>	<a href="#">Dispute Item</a>		
Name: [REDACTED] Date Opened: 12/24/2000	Acct #: [REDACTED] Balance: [REDACTED]	Credit Limit: \$ [REDACTED] Past Due: \$0	Date Reported: 05/13/2018 Acct Status: PAYS AS AGREED
<a href="#">Show Details</a>	<a href="#">Dispute Item</a>		

**Closed Accounts**

Name: [REDACTED] Date Opened: 12/01/2005	Acct #: [REDACTED] Balance: \$0	Credit Limit: \$ [REDACTED] Past Due: \$0	Date Reported: 09/01/2009 Acct Status: PAYS AS AGREED
<a href="#">Show Details</a>	<a href="#">Dispute Item</a>		
Name: [REDACTED] Date Opened: 05/01/2005	Acct #: [REDACTED] Balance: \$0	Credit Limit: \$ [REDACTED] Past Due: \$0	Date Reported: 02/01/2009 Acct Status: PAYS AS AGREED
<a href="#">Show Details</a>	<a href="#">Dispute Item</a>		
Name: [REDACTED] Date Opened: 09/01/1989	Acct #: [REDACTED] Balance: \$0	Credit Limit: \$ [REDACTED] Past Due: \$0	Date Reported: 10/18/2017 Acct Status: PAYS AS AGREED
<a href="#">Show Details</a>	<a href="#">Dispute Item</a>		
Name: [REDACTED] Date Opened: 01/21/2007	Acct #: [REDACTED] Balance: \$0	Credit Limit: \$ [REDACTED] Past Due: \$0	Date Reported: 09/25/2016 Acct Status: PAYS AS AGREED
<a href="#">Show Details</a>	<a href="#">Dispute Item</a>		
Name: [REDACTED] Date Opened: 03/11/1998	Acct #: [REDACTED] Balance: \$0	Credit Limit: \$ [REDACTED] Past Due: \$0	Date Reported: 09/22/2015 Acct Status: PAYS AS AGREED
<a href="#">Show Details</a>	<a href="#">Dispute Item</a>		

95. Equifax represents that the credit information provided through the online dispute portal is “a current copy of your file and has the latest information available.” In other words, the *full content* of a consumer’s credit file, including *all the consumer data that financial institutions furnish to Equifax*, is available once the online dispute portal is accessed. By entering through the dispute resolution portal, it is possible that the hacker had access to consumers’ complete credit files.

96. The dispute resolution portal website runs on Apache Struts software, a popular programming framework for building web applications in Java. Apache Struts makes it “easier

for developers to build top-to-bottom custom websites” and it “can handle everything from interactive screens and logins, to web apps and database management.”<sup>82</sup> Apache Struts is “open source,” meaning that the source code is made freely available and may be redistributed and modified by anyone who wants to use it.

97. While Apache Struts has been widely used by companies and government agencies for years, and is currently in use by at least 65% of Fortune 100 companies,<sup>83</sup> its popularity and expansive capabilities leave it vulnerable to cyberattacks. Indeed, because the software “touches all aspects of a company’s website,” once hackers locate a vulnerability, they gain “unfettered access” to the underlying system and can “execute commands just like they were the administrators.” In other words, “they basically control the system.”<sup>84</sup>

98. According to a report in the *Wall Street Journal*, the vulnerability in Apache Struts “would allow hackers to break into a company by sending data to a server that was specially crafted to take advantage of the flaw. It was the digital equivalent of popping open a side window to sneak into a building.”<sup>85</sup>

99. Once discovered, the potential vulnerability of the Apache Struts software was widely announced so that users of the software could remediate the vulnerability. In March 2017, several entities, including The Apache Foundation, the U.S. Department of Commerce’s National Institute of Standards and Technology (“NIST”), and the U.S. Department of Homeland Security’s Computer Emergency Readiness Team (“U.S. CERT”), issued public warnings regarding the

---

<sup>82</sup> Ben Popken, *Equifax Hackers Exploited Months-Old Flaw*, NBC NEWS (Sept. 14, 2017), <https://www.nbcnews.com/business/consumer/how-did-equifax-hack-even-happen-n801331>.

<sup>83</sup> Keith Collins, *The Hackers Who Broke into Equifax Exploited a Flaw in Opensource Server Software*, QUARTZ (Sept. 8, 2017), <https://qz.com/1073221/thehackers-who-broke-into-equifax-exploited-a-nine-year-old-security-flaw/>.

<sup>84</sup> See Popken, *supra* n.82.

<sup>85</sup> Andriotis *et al.*, *‘We’ve Been Breached’: Inside the Equifax Hack*, *supra* n.3.



vulnerability. The Apache Foundation and NIST described the flaw as “critical,” which is the highest rating those groups use to indicate the danger of a vulnerability.

100. On March 7, 2017, the same day the vulnerability was publicly announced, The Apache Foundation also made available various patches and workarounds to protect against the vulnerability.<sup>86</sup>

101. After this vulnerability was publicly identified, media reports indicated that hackers already were exploiting the vulnerability against various companies and government agencies.<sup>87</sup>

102. Equifax publicly stated that its security team “was aware of this vulnerability [with Apache Struts] at that time [in March 2017].”<sup>88</sup> On March 8, 2017, U.S. CERT sent Equifax a notice of the need to patch a particular vulnerability in the “Apache Struts” software.<sup>89</sup> Equifax admitted that it received the U.S. CERT notification and disseminated it on March 9, 2017.<sup>90</sup>

103. Equifax even knew that patches for the vulnerability were available, but Equifax senior management decided not to implement the patch and instead affirmatively decided to continue to use the outdated version of the software for two and a half months without applying the available patches or taking other measures to protect against the flaw.<sup>91</sup>

---

<sup>86</sup> Elizabeth Weise & Nathan Borney, *Equifax Had Patch 2 Months Before Hack and Didn’t Install It, Security Group Says*, USA TODAY (Sept. 14, 2017), <https://www.usatoday.com/story/money/2017/09/14/equifax-identity-theft-hackers-apache-struts/665100001/>.

<sup>87</sup> Dan Goodin, *Critical Vulnerability Under “Massive” Attack Imperils High-impact Sites*, ARSTECHNICA (Mar. 9, 2017), <https://arstechnica.com/information-technology/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/>.

<sup>88</sup> *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, *supra* n.81.

<sup>89</sup> *Smith Testimony*, *supra* n.1, at 2–3.

<sup>90</sup> *Id.*

<sup>91</sup> George Leopold, *Equifax Ignored Apache Struts Patch For Months*, ENTERPRISETECH (Sept. 15, 2017), <https://www.enterprisetech.com/2017/09/15/equifax-ignored-apache-struts-patch-months/>; *see also* The Apache Software Foundation, *MEDIA ALERT: The Apache Software Foundation Confirms Equifax Data Breach Due to Failure to Install Patches Provided for*

104. Equifax admits that it ran security scans on March 15, 2017, that could have alerted Equifax to the Apache Struts vulnerability. However, because certain key systems did not have proper security certificates, Equifax failed to scan all of its systems and therefore did not discover the Apache Struts vulnerability.<sup>92</sup>

105. Security certificates are designed to secure data that is transmitted between two systems through the use of encryption. There are two main protocols for security certificates, Secure Socket Layer (“SSL”) and Transport Layer Security (“TLS”). Both SSL and TLS allow systems to transmit encrypted information, authenticate that the system is what it claims to be (as opposed to being a server or system used by a malicious third party), and ensure that the systems are communicating with known and authenticated systems. Software tools that scan systems and applications to identify vulnerabilities cannot work on web portals with expired security certificates.<sup>93</sup> Therefore, because Equifax did not properly update its security certifications and allowed its security certificates to expire, Equifax’s scans failed to identify the Apache Struts vulnerability.

---

*Apache® Struts™ Exploit*, THE APACHE SOFTWARE FOUNDATION BLOG (Sept. 14, 2017), <https://blogs.apache.org/foundation/entry/media-alert-the-apache-softwarez> [hereinafter *The Apache Software Foundation, MEDIA ALERT*].

<sup>92</sup> Equifax: Continuing to Monitor Data-Broker Cybersecurity: Hearing Before the SubComm. On Privacy, Technology and the Law of the S. Comm. On the Judiciary, 115<sup>th</sup> Cong. (2017), (Equifax’s Submission in Response to Subcommittee’s Requests Dated October 11, 2017), <https://www.judiciary.senate.gov/imo/media/doc/Smith%20Responses%20to%20QFRs2.pdf> [hereinafter *Equifax’s Oct. 11, 2017 Responses*].

<sup>93</sup> For example, Symantec offers as part of its security certificates free malware scanning to detect potential vulnerabilities. *See Malware Scanning*, Symantec, <https://www.websecurity.symantec.com/security-topics/malware-scanning> (last accessed May 30, 2018).

106. Equifax admits that its systems were breached on May 13, 2017, well over two months after Equifax should have patched the Apache Struts vulnerability.<sup>94</sup> Equifax also acknowledges the unpatched vulnerability in the Apache Struts software allowed hackers to access PII.<sup>95</sup>

107. Between May 13 and July 30, 2017, hackers utilized simple commands to identify the credentials of network accounts at Equifax, allowing them to traverse multiple databases to access and infiltrate the sensitive personal information, including names, Social Security numbers, birth dates, addresses, and driver's license numbers, of approximately 147.9 million U.S. consumers.<sup>96</sup>

108. Indeed, shortly after Equifax publicly announced the Data Breach at issue, security researchers discovered that one of Equifax's online employee portals could be accessed by using the word "admin" for both the login and password. Once logged in through the portal, a hacker could easily access sensitive employee and consumer data.<sup>97</sup>

109. In addition to compromising the PII, the hackers accessed 209,000 consumer credit card numbers, and an estimated 182,000 dispute records containing additional personal information.<sup>98</sup> Equifax stated that it believes all consumer credit card numbers were accessed in one fell swoop in mid-May 2017.

---

<sup>94</sup> *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, *supra* n.81.

<sup>95</sup> *Smith Testimony*, *supra* n.1, at 2–3.

<sup>96</sup> AnnaMaria Andriotis & Robert McMillan, *Hackers Entered Equifax Systems in March*, THE WALL STREET JOURNAL (Sept. 20, 2017), <https://www.wsj.com/articles/hackers-entered-equifax-systems-in-march-1505943617>; Andriotis, *Equifax Identifies Additional 2.4 Million Affected by 2017 Breach*, *supra* n.80.

<sup>97</sup> See Brian Krebs, *Ayuda! (Help!) Equifax Has My Data!*, KREBS ON SECURITY (Sept. 17, 2017), <https://krebsonsecurity.com/2017/09/ayuda-help-equifax-has-my-data/>.

<sup>98</sup> Equifax Inc., Annual Report (Form 10-K) (Mar. 1, 2018) at 2 & 34.

110. On September 11, 2017, Visa issued a CAMS alert of a potential network intrusion at Equifax that put Visa accounts at risk. The Visa CAMS alert indicated that the exposure window was approximately November 10, 2016 through July 6, 2017 and that the debit and credit card data compromised included PAN, CVV2, expiration dates, and cardholder names. Visa further stated that financial institutions receiving the CAMS alert should take necessary steps to prevent fraud and safeguard cardholders.

111. On September 11, 2017, MasterCard issued an ADC alert of a potential network intrusion at Equifax that put MasterCard accounts at risk. The MasterCard ADC alert indicated that the exposure window was approximately November 10, 2016 through July 6, 2017 and that the debit and credit card data compromised included account number and expiration date.

112. In a statement posted September 14, 2017, The Apache Software Foundation attributed the Equifax Data Breach to a single cause: Equifax's "failure to install the security updates provided in a timely manner,"<sup>99</sup> despite being notified about the vulnerabilities in Apache Struts.

113. On October 2, 2017, Equifax announced that Mandiant had completed its internal forensic analysis of the Data Breach. Mandiant determined that an additional 2.5 million consumer records may have been compromised, bringing the total number of potentially compromised accounts to 145.5 million.

114. On November 7, 2017, Visa issued an updated CAMS alert stating that the exposure window had been expanded to August 20, 2016 through July 6, 2017. The updated alert identified the debit and credit card data compromised as PAN, expiration date, cardholder name, cardholder address, Social Security number, and cardholder zip code.

---

<sup>99</sup> The Apache Software Foundation, MEDIA ALERT, *supra* n.91.

115. On November 20, 2017, MasterCard issued an updated ADC alert. The updated alert indicated that the exposure window was approximately August 10, 2016 through September 8, 2017 and that the compromised debit and credit card data included account number, expiration date, Social Security number or equivalent cardholder name and cardholder address.

116. On March 1, 2018, Equifax announced that 2.4 million more U.S. consumers were impacted by the Data Breach than previously disclosed, bringing the total number of potentially compromised accounts to 147.9 million.<sup>100</sup> These additional consumers had names and partial driver's license numbers stolen, according to reports.<sup>101</sup>

117. On May 7, 2018, Equifax submitted a "statement for the record" to the SEC more fully detailing the breakdown of stolen PII.<sup>102</sup>

Information Stolen	Approximate Number of Impacted U.S. Customers
Name	146.6 million
Date of Birth	146.6 million
Social Security Number	145.5 million
Address Information	99 million
Gender	27.3 million
Phone Number	20.3 million
Driver's License Number	17.6 million
Email Address	1.8 million
Payment Card Number and Expiration Date	209,000
Tax ID	97,500
Driver's License State	27,000

<sup>100</sup> Andriotis, *Equifax Identifies Additional 2.4 Million Affected by 2017 Breach*, *supra* n.80.

<sup>101</sup> *Id.*

<sup>102</sup> Equifax Inc., 2016 Form 8-K (May 7, 2018) at 2.

118. Equifax also reported that, in addition to the PII that was previously identified as stolen in the Data Breach, customers' passports, taxpayer identification cards, state identification cards, resident alien cards, and military identification cards were also stolen.<sup>103</sup> These items were required by Equifax and were provided by customers who submitted scans of their ID cards to verify their identity in connection with the online dispute portal.<sup>104</sup>

### **Equifax Delayed Publicly Announcing the Data Breach**

119. Equifax reportedly discovered this Data Breach on July 29, 2017, over four and a half months after U.S. CERT issued a notification about the Apache Struts vulnerability, when Equifax's security team noticed "suspicious network traffic" connected to its consumer dispute portal website.<sup>105</sup>

120. Equifax's security department continued investigating the abnormal activity and, on July 30, 2017, determined that the intrusion was serious enough that the consumer dispute portal website needed to be taken entirely offline.<sup>106</sup>

121. Equifax's CEO Richard Smith was informed of the Data Breach the following day, on July 31, 2017.<sup>107</sup>

122. While Equifax would not disclose the Data Breach to the public for several more weeks, Equifax senior management profited, selling stock or exercising options worth \$2.7 million. On August 1, 2017, only three days after Equifax discovered the Data Breach, Equifax Chief Financial Officer John Gamble sold \$946,374 worth of stock, and President of U.S. Information Solutions Joseph Loughran exercised options to sell \$584,099 worth of stock. The

---

<sup>103</sup> *Id.* at 3.

<sup>104</sup> *Id.*

<sup>105</sup> *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes, supra* n.81.

<sup>106</sup> *Id.*

<sup>107</sup> *Smith Testimony, supra* n.1, at 3.

next day, President of Workforce Solutions Rodolfo Ploder sold \$250,458 worth of stock, and Chief Information Officer Jun Ying sold \$950,000 worth of stock.<sup>108</sup> None of those transactions were part of previously scheduled Rule 10b5-1 trading plans.

123. On August 2, 2017, Equifax informed the Federal Bureau of Investigation (“FBI”) about the Data Breach and retained the law firm of King & Spalding LLP to guide its investigation of the Data Breach. Equifax also hired the cybersecurity forensic firm Mandiant to analyze and investigate the suspicious activity on its network.

124. Over the next several weeks, Mandiant and Equifax’s internal security department analyzed forensic data to determine the nature and scope of the suspicious activity. The investigators determined that Equifax had been subject to cyber-intrusions that resulted in a breach of Equifax’s IT systems.

125. Equifax did not notify its chairman of its board of directors about the Data Breach until August 22, 2017, and waited two more days to inform the full board of directors.

126. Equifax finally publicly revealed the Data Breach on September 7, 2017. But not only did Equifax delay its public announcement for forty days after it learned of the Data Breach, it also soundly botched the next steps in its breach response program.

127. To handle consumer inquiries after the public announcement, Equifax created a website, <https://www.equifaxsecurity2017.com/>, to enable consumers to determine whether they were potentially impacted by the Data Breach. In order to determine whether they were affected, Equifax required consumers to provide their last names and the last six digits of their Social Security numbers. In essence, Equifax required customers potentially harmed by the Data Breach

---

<sup>108</sup> Anders Melin, *Three Equifax Managers Sold Stock Before Cyber Hack Revealed*, BLOOMBERG.COM (Sept. 7, 2017), <https://www.bloomberg.com/news/articles/2017-09-07/three-equifaxexecutives-sold-stock-before-revealing-cyber-hack>.



to provide Equifax with additional sensitive information in order to determine whether their already-provided sensitive information was stolen through the Data Breach.

128. After consumers provided their sensitive information, Equifax's website displayed whether the inquirer was impacted. Under the notice, Equifax's webpage directed consumers to a free identity theft protection and credit monitoring program, TrustedID (a wholly owned subsidiary of Equifax). Equifax offered the identity theft protection and credit monitoring services in the wake of the Data Breach. However, by signing up for TrustedID, consumers consented, often unknowingly, to settle all claims arising out of the use of TrustedID in arbitration. After public outrage over the waiver, Equifax claimed its waiver did not extend to harm caused by the Data Breach.

129. After permitting what is likely to be one of the most damaging data breaches in history, Equifax continued to severely mismanage its websites. Starting on September 9, 2017, Equifax erroneously directed consumers to a fake website at least four times via Twitter.<sup>109</sup> Rather than directing consumers to <https://www.equifaxsecurity2017.com/> (Equifax's legitimate website created to determine whether consumer sensitive information was potentially compromised), Equifax mistakenly directed its Twitter followers to <http://www.securityequifax2017.com/>, a faux version of Equifax's website.

130. On September 15, 2017, Equifax announced the retirements of its Chief Information Officer and Chief Security Officer in connection with the Data Breach and its

---

<sup>109</sup> Janet Burns, *Equifax Was Linking Potential Breach Victims On Twitter To A Scam Site*, FORBES.COM (Sept. 21, 2017), <https://www.forbes.com/sites/janetwburns/2017/09/21/equifax-was-linking-potential-breach-victims-on-twitter-to-a-scam-site/#bb68b87288f2>.

aftermath.<sup>110</sup> Soon after, on September 26, 2017, Equifax announced the retirement of its CEO, Richard Smith, less than three weeks after Equifax disclosed the Data Breach to the public.<sup>111</sup>

### **Post-Breach Investigations Reveal Equifax's Data Security Deficiencies**

131. As a result of its investigation, Equifax identified deficiencies in its patch management policies and protocols that required immediate updates. To resolve its deficiencies, Equifax stated: "Vulnerability scanning and patch management processes and procedures have been enhanced, including an improvement to Equifax's patching procedures to require a 'closed loop' confirmation, which is applied to necessary patches."<sup>112</sup> In addition, the investigation revealed that Equifax entirely lacked adequate monitoring systems and controls necessary to detect the unauthorized infiltration and subsequent exfiltration of consumer data.

132. Senator Elizabeth Warren launched an investigation into the Equifax Data Breach and issued a report in February 2018, entitled *Bad Credit: Uncovering Equifax's Failure to Protect American's Personal Information* (the "Warren Report").<sup>113</sup> Senator Warren's investigation specifically found that Equifax "failed to take adequate steps to prevent the Data Breach" and that Equifax's information and security systems' suffered from numerous material deficiencies.

133. The Warren Report determined that Equifax adopted weak cybersecurity measures that failed to protect consumer data, and that such shortcomings were "a symptom of what appeared to be the low priority afforded cybersecurity by company leaders."<sup>114</sup>

---

<sup>110</sup> *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, *supra* n.81.

<sup>111</sup> Hamza Shaban, *Equifax CEO Richard Smith Steps Down Amid Hacking Scandal*, WASHINGTON POST (Sept. 26, 2017), <https://www.washingtonpost.com/news/the-switch/wp/2017/09/26/equifax-ceo-retires-following-massive-data-breach/>.

<sup>112</sup> Equifax's Oct. 11, 2017 Responses, at 5, *supra* n.92.

<sup>113</sup> Warren Report, *supra* n.58.

<sup>114</sup> *Id.*

134. The Warren Report noted that despite record profits in recent years, Equifax spent only a fraction of its budget on cybersecurity – approximately 3 percent of its operating revenue over the past three years.<sup>115</sup> While Equifax’s data security measures went underfunded, its shareholders profited handsomely. Equifax ultimately paid nearly twice as much in dividends to shareholders over the past three years than it spent on data security.<sup>116</sup>

135. The Warren Report, through consultation with cybersecurity experts, identified six weaknesses in Equifax’s cybersecurity:

a. ***Faulty Patch Management Procedures*** – “For many vulnerabilities that arise in its software and applications, Equifax only has to deploy a software ‘patch’ that will fix the vulnerability and restrict access to the susceptible system . . . Yet Equifax let numerous software vulnerabilities sit un-patched for months at a time, leaving weakness through which hackers could gain access.”

b. ***Feeble Monitoring of Endpoint and Email Security*** – Endpoint security refers to protecting a corporate network when it is accessed via remote devices like laptops and mobile devices, as such devices can create a potential entry point for security threats. “Equifax failed to adopt strict endpoint and email security measure” to secure each endpoint on the network created by these devices.

c. ***Exposure of Sensitive Information*** – Equifax stored and “retained sensitive consumer information on easily accessible system” rather than segregating the most sensitive information into locations designed to limit access and maximize security.

d. ***Weak Network Segmentation*** – Equifax “failed to put security measures in place that would prevent hackers from jumping from insecure, internet-facing systems to backend databases that contain more valuable data. . . . Equifax’s network segmentation measures failed to keep hackers from accessing consumer information because the company did not adopt adequately strict measures to protect valuable data.”

e. ***Inadequate Credentialing*** – “Equifax’s cybersecurity failures extended to their internal security. Each user on Equifax’s system receives a set of privileges. Under strict security standards, Equifax would limit access to the most critical databases to just a handful of necessary users. This would protect the company from internal attacks and further bolster the company’s overall data security regime. After gaining access to Equifax’s systems, hackers then acquired user credentials – a username and password – and accessed a huge quantity of sensitive information using just those credentials. The

---

<sup>115</sup> *Id.*

<sup>116</sup> *Id.*

company did not adopt adequately strict security measures to properly restrict user access to sensitive data.”

f. ***Inadequate Logging*** – “Equifax neglected the use of robust logging techniques that could have allowed the company to expel the hackers from their systems and limited the size and scope of the data breach. Logging is a simple but crucial cybersecurity technique in which companies monitor their systems, continuously logging network access in order to identify unauthorized users. . . . Equifax allowed hackers to continuously access sensitive data for over 75 days, in part because the company failed to adopt effective logging techniques and other security measures.”<sup>117</sup>

136. These findings by the Warren Report demonstrate that Equifax failed to comply with industry standards of care, as well as federal and state laws requiring the protection of consumer data.

137. Equifax’s failures to adopt these industry-standard measures were more than mere mistakes; they were calculated decisions by Equifax executives to skirt data security in favor of paying out annual dividends. As noted in the Warren Report, “Equifax’s goal, as stated by its CEO just weeks before he disclosed the Data Breach, was to go from ‘\$4 billion in revenue to \$8 billion’ in approximately 5 years. Equifax prioritized growth and profits—but did not appear to prioritize cybersecurity.”<sup>118</sup>

138. Former Equifax employees who worked on or alongside the Equifax security team agreed that Equifax did not place a high priority on data security. When asked about Equifax’s data security risk tolerance, a former employee, who worked in IT at Equifax and is now a cybersecurity engineer, stated: “The degree of risk [Equifax] assumes is found, by most of the IT staff who worked elsewhere, to be preposterous.”<sup>119</sup> Another former employee recounted how a 2016 Deloitte security audit found several problems including a careless approach to patching

---

<sup>117</sup> *Id.* at 3–4.

<sup>118</sup> *Id.*

<sup>119</sup> Lorenzo Franceschi-Bicchierai, *Equifax Was Warned*, *supra* n.69; *see also* Cox, *Equifax Suffers Another Security Breach*, *supra* n.73.

systems. According to the employee: “Nobody took that security audit serious[ly] . . . . Every time there was a discussion about doing something, we had a tough time to get management to understand what we were even asking.”<sup>120</sup> Another former Equifax employee commented: “It’s a strange company. Given the amount of data they have access to and the sensitivity to us, security isn’t at the forefront of everybody’s mind, not how it should be.”<sup>121</sup>

139. Equifax’s Data Breach spawned several additional investigations. For example, federal regulators investigated Equifax’s delayed notification about the Data Breach; the FBI is investigating the cause and extent of the Data Breach; and, Congress has held at least a half a dozen committees’ hearings on Equifax’s Data Breach.<sup>122</sup>

140. Numerous state attorneys general rebuked Equifax in the wake of the Data Breach. On September 18, 2017, New York Governor Andrew Cuomo directed the state’s Department of Financial Services to develop a rule forcing credit reporting agencies to register with the state and comply with its cybersecurity requirements.<sup>123</sup> On September 19, 2017, attorneys general from 43 states and the District of Columbia signed a letter to Equifax, criticizing it for the Data Breach and its response.<sup>124</sup> The same day, Massachusetts Attorney General Maura Healey filed a suit against Equifax, seeking financial penalties and disgorgement of profits, alleging that Equifax failed to

---

<sup>120</sup> *Id.*

<sup>121</sup> *Id.*

<sup>122</sup> Andriotis & McMillan, *Hackers Entered Equifax Systems in March*, *supra* n.96.

<sup>123</sup> Ashley Southall, *Cuomo Proposes Stricter Regulations for Credit Reporting Agencies*, NEW YORK TIMES (Sept. 18, 2017), <https://www.nytimes.com/2017/09/18/nyregion/equifax-hack-credit-reporting-agencies-regulations.html>.

<sup>124</sup> Jack Suntrup, *Hawley, Madigan Criticize Equifax in Letter Signed by Other State Attorneys General*, ST. LOUIS POST-DISPATCH (Sept. 19, 2017), [http://www.stltoday.com/business/national-and-international/hawley-madigan-criticize-equifax-in-letter-signed-by-other-state/article\\_868a0dbf-1ec6-57e0-87a7-6d008005f8f0.html](http://www.stltoday.com/business/national-and-international/hawley-madigan-criticize-equifax-in-letter-signed-by-other-state/article_868a0dbf-1ec6-57e0-87a7-6d008005f8f0.html).

promptly notify the public of the Data Breach, failed to protect the personal data in its possession, and engaged in unfair and deceptive trade practices.<sup>125</sup>

141. Equifax’s Data Breach is likely to be one of the most damaging data breaches in history, measured by both the sheer number of people exposed and the sensitivity and composition of the PII compromised: “[t]he Equifax hack is potentially the most dangerous of all, though, because the attackers were able to gain vast quantities of PII – names, addresses, Social Security numbers and dates of birth – at one time.”<sup>126</sup>

142. Ultimately, the Equifax Data Breach was the result of a top-down policy to prioritize growth and profits over data security. As Equifax’s CEO admitted, Equifax did not reduce the scope of sensitive data retained in backend databases.<sup>127</sup> The technical deficiencies and weaknesses that permitted unfettered access to Equifax’s systems demonstrate the low priority Equifax gave to even rudimentary data security protocols, despite Equifax’s role as one of the largest custodians of consumer data in the world.

143. Equifax did not employ reasonable measures that are critical to data security, including: vulnerability scanning and patch management processes and procedures; restrictions and controls for accessing critical databases; network segmentation between internet facing systems and backend databases and data stores; firewalls; file integrity monitoring; network,

---

<sup>125</sup> David Lynch, *Equifax Faces Legal Onslaught from US States*, FINANCIAL TIMES (Sept. 21, 2017), <https://www.ft.com/content/bf04768c-9e1b-11e7-8cd4-932067fbf946>.

<sup>126</sup> AnnaMaria Andriotis, Robert McMillan, & Christina Rexrode, *Equifax Hack Leaves Consumers, Financial Firms Scrambling*, THE WALL STREET JOURNAL (Sept. 8, 2017), <https://www.wsj.com/articles/equifax-hack-leaves-consumers-financial-firms-scrambling-1504906993>.

<sup>127</sup> Equifax’s Oct. 11, 2017 Responses, *supra* n.92.

application, database, and system-level logging to monitor the network for unusual activity; and endpoint detection software to prevent exfiltration of data.<sup>128</sup>

144. But even the existence of these major security deficiencies does not explain how hackers were able to move around Equifax's servers unnoticed for more than 75 days while exfiltrating hundreds of millions of consumer records. Indeed, any routine and competent monitoring would have revealed to Equifax that there was significant irregular activity taking place on its servers.

145. Only now, after the damage has been done, has Equifax devoted the resources it originally should have earmarked to safeguard PII. In fact, as of March 31, 2018, Equifax recorded \$113.3 million of pretax expenses related to the Data Breach.<sup>129</sup>

#### **Equifax Failed to Comply with Industry Standards of Care as to Data Security**

146. Equifax fully understood its duties to protect the confidentiality, accuracy, and integrity of PII. It serves as a linchpin of the U.S. economy, enabling financial institutions, like Plaintiff and the Class, to extend credit and other financial services to U.S. consumers. It heralds itself as a "trusted steward" that is compliant with the laws requiring Equifax to adequately safeguard consumer data. In fact, however, Equifax violated federal and state data security requirements and disregarded reasonable data security standards of care.

147. One such reasonable data security standard of care is the NIST Guide to Enterprise Patch Management Technologies.<sup>130</sup> NIST develops standards and guidelines for the cost-effective security and privacy of information (other than national security-related information) for

---

<sup>128</sup> *Smith Testimony, supra* n.1.

<sup>129</sup> Equifax Inc., Quarterly Report (Form 10-Q) (April 26, 2018) at 19.

<sup>130</sup> Murugiah Souppaya and Karen Scarfone, *Guide to Enterprise Patch Management Technologies*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (July 2013), <http://dx.doi.org/10.6028/NIST.SP.800-40r3>.



the federal government. The NIST Guide to Enterprise Patch Management Technologies advises organizations to timely implement patches because they “correct security and functionality problems in software and firmware. From a security perspective, patches are most often of interest because they are mitigating software flaw vulnerabilities; applying patches to eliminate these vulnerabilities significantly reduces the opportunities for exploitation.”<sup>131</sup> Moreover, the NIST Guide to Enterprise Patch Management Technologies advises that “[o]rganizations should use other methods of confirming [patch] installation, such as a vulnerability scanner that is independent from the patch management system.”<sup>132</sup>

148. The NIST also has published a Guide to Application Whitelisting for computer security, which states that “application whitelisting software prevents installation and/or execution of any application that is not specifically authorized for use on a particular host. This mitigates multiple categories of threats, including malware and other unauthorized software.”<sup>133</sup> NIST further recommends that “[o]rganizations should consider [application whitelisting] technologies, particularly for centrally managed desktops, laptops, and servers, because of the relative ease in managing these solutions and the minimal additional cost.”<sup>134</sup>

149. The International Standards Organization (“ISO”) and the International Electrotechnical Commission (“IEC”) likewise have developed standards relating to information security management systems. ISO/IEC 27001 provides a checklist and comprehensive control

---

<sup>131</sup> *Id.*

<sup>132</sup> *Id.*

<sup>133</sup> Adam Sedgewick, Murugiah Souppaya, and Karen Scarfone, *Guide to Application Whitelisting*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Oct. 2015), <http://dx.doi.org/10.6028/NIST.SP.800-167>.

<sup>134</sup> *Id.* at 5.

objectives for information security policies that guide organizations in protecting their information systems and networks.<sup>135</sup> Specifically, the control objectives include:

**A.5.1 Information Security Policy:** Objective: to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

**A.6.1.1 Management Commitment to Information Security:** Control – Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

**A.10.3 System planning and acceptance:** Objective: To minimize the risk of systems failures.

**A.10.3.2 System acceptance:** Control – Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.

**A.10.4 Protection against malicious and mobile code:** Objective: To protect the integrity of software and information.

**A.10.4.1 Controls against malicious code:** Control – Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.

**A.10.6 Network security management:** Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.

**A.10.6.1 Network controls:** Control – Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

**A.10.10 Monitoring:** Objective: To detect unauthorized information processing activities.

**A.10.10.1 Audit logging:** Control – Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.

**A.11.4 Network access control:** Objective: To prevent unauthorized access to networked services.

---

<sup>135</sup> ISO/IEC 27001 (2005), available at [http://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/adeaf3e5\\_cc55\\_4222\\_8767\\_f26bcaec3f70/ISO\\_IEC\\_27001.pdf](http://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/adeaf3e5_cc55_4222_8767_f26bcaec3f70/ISO_IEC_27001.pdf).

**A.11.4.1 Policy on use of network services:** Control – Users shall only be provided with access to the services that they have been specifically authorized to use.

**A.11.4.7 Network routing control:** Control – Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

**A.12.4 Security of system files:** Objective: To ensure the security of system files.

**A.12.4.1 Control of operational software:** Control – There shall be procedures in place to control the installation of software on operational systems.

**A.13.1 Reporting information security events and weaknesses:** Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

**A.13.1.1 Reporting information security events:** Control – Information security events shall be reported through appropriate management channels as quickly as possible.<sup>136</sup>

150. Similarly, ISO/IEC 27002 provides additional, specific best practice recommendations on information security management systems.<sup>137</sup> For example, ISO/IEC 27002 states that in order to properly protect against malicious and mobile code and to protect the integrity of software and the organization's information, the following guidance should be observed:

Implementation guidance: Protection against malicious code should be based on malicious code detection and repair software, security awareness, and appropriate system access and change management controls.

151. As discussed herein, Equifax failed to comply with the foregoing industry standards.

**Plaintiff and the Class Have Been, and Will Continue to Be, Harmed by the Equifax Data Breach**

---

<sup>136</sup> *Id.* at 13-26.

<sup>137</sup> ISO/IEC 27002 (2005), available at <http://www.slinfo.una.ac.cr/documentos/EIF402/ISO27001.pdf>.

152. Plaintiff and the Class provide consumers with a wide range of financial services, including deposit accounts, loans, and credit or debit cards. As direct participants in the country's financial services and credit reporting system, Plaintiff and the Class both contribute and receive confidential consumer information, all of which is comprised of and/or is associated with consumers' PII. Because the vast quantity of consumer data compromised as a result of the Data Breach is the same consumer data Plaintiff uses to conduct their business, Plaintiff and the Class have suffered and are at increased risk of suffering losses as a result of various forms of fraudulent banking activity.

153. In response to the public announcement of the Equifax Data Breach, Plaintiff and the Class have been and will continue to be subjected to a greater risk of fraudulent banking activity. They have been obligated to investigate the impact of the Equifax Data Breach on their financial institutions and their customers and have needed to implement appropriate additional measures to mitigate the risk of fraudulent banking activity. As a direct result of the Equifax Data Breach, Plaintiff and the Class have suffered, and will continue to suffer, tangible and intangible harm, including, *inter alia*: (a) direct out of pocket costs to reimburse customers and costs related to investigating the impact of the Equifax Data Breach, evaluating existing and alternative security protocols, monitoring for potentially fraudulent banking activity, and communicating with customers regarding their concerns about identity theft and the safety of their accounts held with Plaintiff and the Class; and (b) a certainly impending risk of future harm, in the form of future fraudulent banking activity, as a direct result of the compromised PII associated with the Equifax Data Breach, which will continue into the foreseeable future, and will require Plaintiff and the Class to incur significant costs and expenses in order to reduce and mitigate this risk of harm.

154. According to the American Bankers Association (“ABA”), “[g]iven the scope of the cyberattack, all banks will have a substantial percentage of customers whose information was breached.”<sup>138</sup> According to Oliver Wyman, a management consulting firm, the Equifax Data Breach has profound implications for companies like Plaintiff and the Class, “who use information stored by credit bureaus as a mechanism for confirming the identity of new and returning customers.”<sup>139</sup> It states that “there is a real question as to which commonly used identity-confirmation processes are still viable.”<sup>140</sup> Even standard procedures for confirming identity that require customers to answer challenge questions based on the content of their credit files “are now far less safe as the underlying information has been hacked.”<sup>141</sup>

155. Thus, there is no doubt that Plaintiff and the Class have borne, and will continue to bear, much of the financial impact of dealing with the Equifax Data Breach. One commentator predicts: “Banks are going to pay the most of anyone.”<sup>142</sup> This is because it is ultimately financial institutions that bear the risk of loss if identity thieves open accounts, transfer funds, take out loans, or obtain credit or debit cards.<sup>143</sup> Financial institutions also must reimburse consumers whose PII was compromised in the Data Breach for fraud losses that are incurred in connection with accounts held at their financial institutions. *See, e.g.*, 15 U.S.C. §§1643 & 1693g.

---

<sup>138</sup> Krista Shonk & Nessa Feddis, *Third-Party Tactics: Tips for Managing the Equifax Breach*, ABA BANKING JOURNAL (Nov. 2, 2017), <https://bankingjournal.aba.com/2017/11/third-party-tactics-tips-for-managing-the-equifax-breach/>.

<sup>139</sup> Paul Mee & Chris DeBrusk, *The Equifax Data Breach And Its Impact On Identity Verification*, OLIVER WYMAN (Sept. 2017), [https://www.marsh.com/content/dam/oliver-wyman/v2/publications/2017/sep/Oliver\\_Wyman\\_Equifax\\_Data\\_Breach.pdf](https://www.marsh.com/content/dam/oliver-wyman/v2/publications/2017/sep/Oliver_Wyman_Equifax_Data_Breach.pdf).

<sup>140</sup> *Id.*

<sup>141</sup> *Id.*

<sup>142</sup> Joe Ruben, *BankThink Fallout from Equifax Breach Will Hit Banks Hardest*, AMERICAN BANKER (Sept. 29, 2017), <https://www.americanbanker.com/opinion/fallout-from-equifax-breach-will-hit-banks-hardest>.

<sup>143</sup> *See, e.g., id.*

156. The compromised PII is precisely the data that identity thieves need to wreak havoc throughout the financial services industry, allowing them to illegitimately open accounts, apply for loans, use credit and debit cards, and transfer funds with stolen and synthetic identities.<sup>144</sup>

157. Equifax even acknowledges that this type of harm is a reality for financial institutions when PII is compromised:

Fraudsters can build synthetic identities by creating a fake SSN or obtaining/stealing a real SSN and adding non-matching identifying information such as name, date of birth, and address. Perpetrators often prefer to steal randomized SSNs or purchase them from hackers who breach public or private databases that contain personally identifiable information. Then the fraudster uses the synthetic identity to apply for a line of credit, typically at a bank. The bank submits an inquiry to credit bureaus about the applicant's credit history. The credit bureaus initially report that an associated profile does not exist and the bank may reject the application; however, the credit inquiry generates a credit profile for the synthetic identity in the credit bureaus' databases. At this stage, the perpetrator will typically apply for multiple credit cards and other products marketed to consumers who are new to credit. They maintain good credit over time to build up credit limits and apply for more cards. Most times, the fraudster ends up charging the maximum amount on credit cards and not paying the bill (known as "bust-out" fraud) or they may launder the money between multiple accounts.<sup>145</sup>

158. A report by the Department of Justice found that fraudulent use of existing account information, including credit card and bank account information, affected 86% of identity theft victims in 2014.<sup>146</sup>

159. The Credit Union Executive Society ("CUES") concludes that credit unions and other financial institutions will be subject to increased fraud and well-disguised fraud attempts as a result of the Equifax Data Breach.<sup>147</sup> Specifically, CUES states that because "the stolen

---

<sup>144</sup> See, e.g., *id.*

<sup>145</sup> Donahoo, *How Fraudsters Are Using Synthetic Identities*, *supra* n.2.

<sup>146</sup> Erika Harrell, *Victims of Identity Theft, 2014*, U.S. DEPARTMENT OF JUSTICE, BUREAU OF JUSTICE STATISTICS, NCJ 248991 at 1 (Sept. 2015), <https://www.bjs.gov/content/pub/pdf/vit14.pdf>.

<sup>147</sup> Frank McKenna, *Planning, Post Equifax*, 40 CREDIT UNION MGMT. MAGAZINE (Oct. 2017), available at <https://www.cues.org/article/viewalldd/planning-post-equifax>.

information is personal credit bureau data that lasts a consumers' entire lifetime . . . the foundation that banks and credit unions use to control new account fraud or application fraud is badly damaged.”<sup>148</sup>

160. CUES advises that fraud managers at financial institutions should plan for and adopt heightened fraud detection methods because, as a direct result of the Data Breach: (1) knowledge-based authentication tools will be less effective; (2) increased new account and new loan application fraud will occur; and (3) credit card fraud will increase.<sup>149</sup>

161. The ABA recognizes similar risks and recommends that banks should: (1) assess and analyze the impact of the Data Breach in order to “detect potential risks to the bank and its customers”; (2) enhance account monitoring activities “with a particular emphasis on preventing new account identity theft, synthetic identity theft, and takeover of bank and credit accounts”; (3) anticipate credit report freezes, which “may slow the review of credit applications and create compliance timing complications, particularly for mortgage loans”; and (4) update their identity theft red flag program.<sup>150</sup>

162. Therefore, Plaintiff and the Class were forced to take immediate action in response to the Equifax Data Breach.<sup>151</sup> The operational impact on Plaintiff and the Class has been and will continue to be significant. In light of the magnitude of the Data Breach and the type of PII compromised, Plaintiff and the Class, at a minimum, have incurred costs to investigate the specific impact of the Data Breach on their individual institution, evaluate their authentication policies,

---

<sup>148</sup> *Id.*

<sup>149</sup> *Id.*

<sup>150</sup> Shonk & Feddis, *Third-Party Tactics*, *supra* n.138.

<sup>151</sup> *See, e.g., id.*



protocols, procedures, and measures, and increase monitoring for and awareness of fraudulent banking activity.

163. Furthermore, the repercussions from the Data Breach have been and will continue to be long lasting.<sup>152</sup> According to Nick Clements, who formerly ran a fraud department at Citigroup:

This stuff takes time[.] . . . If names and Social Security numbers and dates of birth are out there, they will be used at some point. No one should take reassurance that a few weeks in, they don't detect a high level of activity. . . . There's a long shelf life here.<sup>153</sup>

### **Authentication**

164. The Equifax Data Breach has had a particularly significant impact on the measures financial institutions use to authenticate new and potential customers. Security experts warn that “the scale of the Equifax breach means that every SSN in the United States – together with the accompanying name – must be presumed to be public knowledge, and thus should not be used to validate anyone's identity, ever again.”<sup>154</sup>

165. As explained in the American Banker:

***This incident may call into question the industry's dependence on consumer data for authentication.***

“Financial institutions and other similar businesses that rely on personally identifiable information are being confronted with an environment where all of this data is being bought and sold, fed by these types of events,” said Al Pascual, senior vice president, research director and head of fraud and security at Javelin Strategy & Research.

---

<sup>152</sup> Penny Crosman, *Seven Aftershocks of the Equifax Breach: What bankers need to know*, AMERICAN BANKER (Sept. 8, 2017), <https://www.americanbanker.com/news/seven-aftershocks-of-the-equifax-breach-what-bankers-need-to-know>; Ruben, *BankThink Fallout from Equifax Breach Will Hit Banks Hardest*, *supra* n.142.

<sup>153</sup> Crossman, *Seven Aftershocks of the Equifax Breach*, *supra* n.152.

<sup>154</sup> Mathew J. Schwartz, *Equifax Breach: 8 Takeaways*, BANK INFO SECURITY (Sept. 8, 2017), <https://www.bankinfosecurity.com/equifax-breach-8-takeaways-a-10278>; *see also* Mee & Chris DeBrusk, *The Equifax Data Breach And Its Impact On Identity Verification*, *supra* n.139.

That means *they can no longer rely strictly on PII any longer as a means of verifying identity*.<sup>155</sup> [Emphasis added].

166. Plaintiff and the Class, at a minimum, have expended resources to assess the impact of the Data Breach and their ability to authenticate current and potential customers. Many have incurred and will continue to incur additional costs to revise their methods of authentication.

### **Fraudulent Banking Activity**

167. The opening of new accounts is a particularly significant risk for financial institutions. As explained in the American Banker:

This breach heightened the risk of fraudulent account openings at a time when banks and fintech companies are increasingly allowing consumers to open new accounts on mobile devices in faster time frames — often in less than 10 minutes.

When banks and fintechs open accounts online, they typically use information provided by credit reporting agencies to help verify identities and meet Bank Secrecy Act obligations, pointed out Scott Sargent, an attorney with Baker Donelson's Financial Services Transactions Group.

“Banks and fintechs will need to closely evaluate their processes in light of the Equifax breach to make sure the information they are getting is still accurately verifying their online customers,” Sargent said.<sup>156</sup>

168. Another commentator confirmed that as a direct result of the Data Breach, financial institutions face an increased risk of new account fraud and the fraudulent transactions that inevitably result:

After the 2017 Equifax hacking scandal, experts say consumers increasingly need to be on the lookout for phantom bank accounts, mysterious credit cards and other gruesome things. And remember, scammers don't walk around in gory masks with fake blood dripping off their teeth.... A phantom account is when someone, not you, opens a bank account in your name using your ID... Ken Tumin, founder and editor of DepositAccounts.com, said sometimes a criminal will open a checking

---

<sup>155</sup> Crossman, *Seven Aftershocks of the Equifax Breach*, *supra* n.152.

<sup>156</sup> *Id.*; see also Mee & Chris DeBrusk, *The Equifax Data Breach And Its Impact On Identity Verification*, *supra* n.139.

account using your ID and then possibly attempt to link to another one of your accounts to try to withdraw money.<sup>157</sup>

169. Thus, Plaintiff and the Class have expended resources to evaluate their methods of monitoring for and preventing fraudulent banking activity, and many have incurred and will continue to incur additional costs to implement new methods of fraud monitoring and prevention.

### **Customer Relations**

170. Plaintiff and the Class have devoted and will continue to devote resources to investigating complaints regarding fraudulent banking activity and assuaging customer concerns about the safety of their financial accounts. Consumers inevitably face significant emotional distress relating to identity theft and the risk of identity theft. According to the Department of Justice, an estimated 36% of identity theft victims experienced moderate or severe emotional distress as a result of the crime.<sup>158</sup> This stress also impacts financial institutions, which are forced to expend additional customer service resources assisting their concerned customers.

### **Regulatory Compliance**

171. Financial institutions also may face increased regulatory compliance costs going forward as a result of the Data Breach. Federal regulators are considering the Data Breach's implications and are likely to implement additional requirements to protect consumers from the financial risks associated with the Data Breach. For example, Plaintiff and the Class will likely be required to provide regulators with additional reports and plans, and will be required to directly bear the administrative costs of any such additional measures.

### **Lost Opportunity Costs and Reputational Harm**

---

<sup>157</sup> Susan Tompor, *Something Evil Lurks in Fake Checks and Phantom Financial Doings*, DETROIT FREE PRESS (Oct. 26, 2017), <https://www.freep.com/story/money/personal-finance/susan-tompor/2017/10/26/fake-checks-phantom-bank-accounts-other-tricks/789905001/>.

<sup>158</sup> Harrell, *Victims of Identity Theft*, 2014, *supra* n.146.

172. Plaintiff and the Class have suffered, and will continue to suffer, lost profits and reputational harm as a result of the Data Breach. In the wake of the Data Breach, Equifax and others have directed consumers to “[c]onsider placing a security freeze . . . on your credit report.”<sup>159</sup> As CRAs acknowledge, however, credit freezes “may delay, interfere with or prohibit the timely approval” of a range of services, including “a new loan, credit, mortgage, insurance, government services or payments, rental housing, employment, investment, license, cellular telephone, utilities, digital signature, Internet credit card transaction or other services, including an extension of credit at point of sale.”<sup>160</sup>

173. Credit freezes can lead to reduced revenues for financial institutions as they are not able to efficiently complete credit applications:

Consumers may freeze their credit reports in an effort to protect against identity theft. These freezes may slow the review of credit applications and create compliance timing complications, particularly for mortgage loans. As a result, banks should review their credit application processes and be prepared to address questions and expectations of customers who have frozen their credit reports.<sup>161</sup>

174. The American Banker recently wrote that the Equifax Data Breach will result in long term added costs and to the activities conducted by financial institutions:

[I]n most cases lenders will likely interpret “better authentication” as requiring more data from consumers to help ensure that the applicant is indeed who he says he is. For example, lenders may ask consumers to respond to more out-of-wallet questions during the application process that are more difficult for an identity thief to answer, like, “What is your mortgage payment?” or “Did you own a certain type of car? This process will require consumers to provide more information to prove their identity. More disclosure of information from consumers will slow down the lending process because consumers may need to gather more information to complete the process and because it will also take them more time to fill in lender requirements. Requiring consumers to disclose more information could lead

<sup>159</sup> 2017 Cybersecurity Incident & Important Consumer Information, EQUIFAX INC., <https://www.equifaxsecurity2017.com/> (last accessed May 30, 2018).

<sup>160</sup> Security Freeze, EXPERIAN INFORMATION SOLUTIONS, INC., <https://www.experian.com/blogs/ask-experian/credit-education/preventing-fraud/security-freeze/> (last accessed May 30, 2018).

<sup>161</sup> Shonk & Feddis, *Third-Party Tactics*, *supra* n.138.

consumers to abandon credit applications that are otherwise supposed to be quick and painless, such as the process for obtaining instant retail credit. Specifically, a less convenient process in addition to heightened consumer fears about their data being hacked could discourage consumers from completing a loan application unless it is a credit line they absolutely must have.<sup>162</sup>

175. Inconvenienced customers often blame Plaintiff and the Class for the frustration associated with added authentication measures.

176. Financial institutions are also harmed by the chilling effect the Data Breach has and will have on consumers' willingness to seek extensions of credit through instruments like home mortgages and credit cards. Customers who do not react to the Data Breach by placing a freeze on their credit, may nevertheless refrain from obtaining credit in the wake of the Data Breach. This results in lost fees and interest to financial institutions.

177. In sum, the Equifax Data Breach has sent shockwaves throughout the entire financial services industry, causing immediate injury and dramatically increasing a certainly impending risk of future harm, in the form of future fraudulent banking activity, in the immediate and foreseeable future to Plaintiff and the Class. Plaintiff and the Class therefore seek damages and injunctive relief for Equifax's negligence, negligence per se, negligent misrepresentation, and violation of state unfair and deceptive trade practices statutes.

### **CLASS ACTION ALLEGATIONS**

178. Plaintiff brings this action on behalf of itself and as a class action under Rules 1702, 1708, and 1709 of the Pennsylvania Rules of Civil Procedure, on behalf of the following class (the "Class"):

All Financial Institutions that are headquartered in Pennsylvania and that do business with consumers whose PII was exposed as a result of the Equifax Data Breach announced on or about September 7, 2017.

---

<sup>162</sup> Ruben, *BankThink Fallout from Equifax Breach Will Hit Banks Hardest*, *supra* n.142.

The Class asserts claims against Equifax for negligence (Count 1) and negligence *per se* (Count 2). The Class also requests a declaratory judgment (Count 3).

179. Excluded from the Class are Equifax, any entity in which Equifax has a controlling interest, and Equifax's officers, directors, legal representatives, successors, subsidiaries, and assigns.

180. **Numerosity – Pa. R. Civ. P. 1702(1).** The members of the Class are so numerous that joinder would be impracticable. According to iBanknet, there are approximately 514 financial institutions based in Pennsylvania.<sup>163</sup>

181. **Commonality and Predominance – Pa. R. Civ. P. 1702(2) and (5) and 1708(a)(1).** There are common questions of law and fact that predominate over questions affecting only individual Class members. These common legal and factual questions include, but are not limited to:

- a. whether Equifax owed a duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and members of the Class when obtaining, storing, using, and managing PII, including taking action to safeguard such data;
- b. whether Equifax actively mishandled PII and implemented and maintained data security measures that it knew or should have known were unreasonable and inadequate to protect PII;
- c. whether Equifax negligently allowed PII to be accessed, used, or disclosed by third parties;

---

<sup>163</sup> See iBanknet, Pennsylvania Financial Institutions, <http://www.ibanknet.com/scripts/callreports/fiList.aspx?type=stateallfi&state=42> (last accessed July 8, 2019).

- d. whether Equifax failed to adequately notify Plaintiff and members of the Class that its data systems were breached;
- e. whether Plaintiff and members of the Class were injured and suffered damages and ascertainable losses;
- f. whether Equifax's actions and inactions failed to provide reasonable security proximately caused the injuries suffered by Plaintiff and members of the Class;
- g. whether Plaintiff and members of the Class are entitled to damages and, if so, the measure of such damages; and
- h. whether Plaintiff and members of the Class are entitled to injunctive, equitable, declaratory and/or other relief, and if so, the nature of such relief.

182. **Typicality – Pa. R. Civ. P. 1702(3).** Plaintiff's claims are typical of the claims of the absent class members and have a common origin and basis. Plaintiff and absent Class members are all financial institutions injured by Equifax's Data Breach. The Plaintiff's claims arise from the same practices and course of conduct giving rise to the claims of the absent Class members and are based on the same legal theories, namely the Equifax Data Breach. If prosecuted individually, the claims of each Class member would necessarily rely upon the same material facts and legal theories and seek the same relief. Plaintiff's claims arise from the same practices and course of conduct that give rise to the other Class members' claims and are based on the same legal theories.

183. **Adequacy – Pa. R. Civ. P. 1702(4) and 1709.** Plaintiff will fully and adequately assert and protect the interests of the absent Class members and have retained Class counsel who are experienced and qualified in prosecuting class action cases similar to this one. Neither Plaintiff



nor its attorneys have any interests contrary to or conflicting with the interests of absent Class members.

184. **Manageability – Pa. R. Civ. P. 1708 (a)(2).** The claims of the Plaintiff and Class members are substantially identical as explained above, certifying the case as a class action will centralize these substantially identical claims in a single proceeding and adjudicating these substantially identical claims at one time is the most manageable litigation method available to Plaintiff and the Class.

185. **Risk of Inconsistent, Varying, or Prejudicial Adjudications – Pa. R. Civ. P. 1708(a)(3).** If the claims of Plaintiff and the members of the class were tried separately, Defendants may be confronted with incompatible standards of conduct and divergent court decisions. Furthermore, if the claims of Plaintiff and the members of the class were tried individually, adjudications with respect to individual class members and the propriety of their claims could be dispositive of the interests of other members of the class not party to those individual adjudications and substantially, if not fully, impair or impede their ability to protect their interests.

186. **Litigation Already Commenced – Pennsylvania Rule of Civil Procedure 1708(a)(4).** A multi-district litigation class action is pending in the Northern District of Georgia, styled as *In re: Equifax Data Security Breach Litig.*, Case No. 1:170md-2800, which involves issues pertaining to Payment Card Data losses. However, Plaintiff has no claims currently pending in that action and no class has been certified yet in that action.

187. **The Appropriateness of the Forum – Pennsylvania Rule of Civil Procedure 1708(a)(5).** This is the most appropriate forum to concentrate the litigation because Plaintiff and

the Class members all reside in the Commonwealth of Pennsylvania and Plaintiff resides in this County. Further, Defendants routinely do business in both this Commonwealth and this County.

188. **The Class Members' Claims Support Certification – Pennsylvania Rule of Civil Procedure 1708(a)(6) and (7).** The expenses of individual litigation are insufficient to support or justify individual suits. Furthermore, the damages that may be recovered by the class will not be so small such that class certification is unjustified.

189. **The General Applicability of Defendant's Conduct – Pennsylvania Rule of Civil Procedure 1708(b)(2).** Defendants' uniform conduct is generally applicable to the class as a whole, making relief appropriate with respect to each class member.

## **LEGAL CLAIMS**

### **COUNT 1**

#### **Negligence**

#### **(On behalf of Plaintiff and the Class)**

190. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

191. Equifax owes a common law duty under Pennsylvania law to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and members of the Class when obtaining, storing, using, selling, and managing PII, including taking action to reasonably safeguard such data and providing notification to Plaintiff and the Class of any breach in a timely manner so that appropriate action can be taken to minimize or avoid losses. This duty arises from several sources (described below) and is independent of any duty Equifax owed as a result of any contractual obligations.

192. This duty extends to protecting others against the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where an actor's own conduct or

misconduct exposes another to the risk or defeats protections put in place to guard against the risk, where the actor is in possession of something valuable that affords a peculiar temptation for criminal interference, or where the parties are in a special relationship. *See* Restatement (Second) of Torts §302B. Numerous courts and legislatures also have recognized the existence of a specific duty to reasonably safeguard PII and other sensitive information.

193. Equifax's sole business purpose is to collect, store, use, maintain, sell, and transmit consumer PII. Equifax holds itself out as one of the three nationwide CRAs that serve as linchpins of the financial system. In this role, Equifax was entrusted with sensitive and valuable PII regarding hundreds of millions of consumers. Plaintiff and the Class, who provide various financial services, including the extension of credit, to the same consumers whose PII was compromised as a result of the Equifax Data Breach, are in a symbiotic relationship with Equifax. Equifax strongly encourages financial institutions to furnish Equifax with their consumer data so that Equifax can provide accurate and reliable information to financial institutions, which rely on the integrity of the credit reporting system to extend credit and provide other financial services.

194. Thus, the common law duty to use reasonable care to avoid causing foreseeable risk of harm exists in this case because Plaintiff and members of the Class were the foreseeable and probable victims of any data breach of Equifax's systems that occurred as a result of Equifax's inadequate data security practices. In fact, Equifax knew it was more likely than not that Plaintiff and members of the Class would be harmed by a breach of Equifax's systems given the closed-universe symbiotic relationship that exists between financial institutions and Equifax. Indeed, Equifax calls itself a "trusted steward" of data and markets numerous fraud and identity theft prevention and protection solutions directly to financial institutions. Equifax also knew that it was

in possession of one of the most valuable collections of data in the world, and that Equifax's systems would therefore be tempting targets for data thieves.

195. It was foreseeable that injury to Plaintiff and the Class would result from Equifax's active mishandling of PII, including, but not limited to, not using reasonable security measures to protect such PII and to provide timely notice of the Data Breach. Indeed, Equifax acknowledged the risk of a data breach and the impact such a breach could have on Equifax, consumers, and financial institutions, like Plaintiff and the Class, in its 2016 Form 10-K filed with the SEC.

196. In the current environment where data breaches are near commonplace (as discussed above), Equifax knew or should have known of the significant risk that its computer systems would be breached, particularly in light of the numerous data breach incidents it experienced prior to the Data Breach.

197. Equifax's duty to act reasonably in managing consumer data and to use reasonable data security measures also arises under the GLBA, 15 U.S.C. §§6801-6809, and its implementing regulations, 16 C.F.R. Part 314 (the "Safeguards Rule"), which "sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information" and "applies to the handling of customer information by all financial institutions over which the [FTC] has jurisdiction." 16 C.F.R. §314.1(a)-(b). Equifax is a financial institution, as defined in Section 509(3)(A) of the GLBA, 15 U.S.C. §6809(3)(A).

198. The Safeguards Rule "applies to all customer information in [a financial institution's] possession, regardless of whether such information pertains to individuals with whom [a financial institution has] a customer relationship, or pertains to the customers of other

financial institutions that have provided such information to [the subject financial institution].” 16 C.F.R. §314.1(b).

199. The Safeguards Rule requires financial institutions to “develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to [the financial institution’s] size and complexity, the nature and scope of [the financial institution’s] activities, and the sensitivity of any customer information at issue.” 16 C.F.R. 314.3(a).

200. Specifically, the Safeguards Rule requires a financial institution, among other things, to:

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) Employee training and management;

(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

\* \* \*

(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this

section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program. 16 C.F.R. 314.4.

201. As alleged herein, Equifax breached its duties under the GLBA. The security program and safeguards Equifax maintained were not appropriate to Equifax's size and complexity, the nature and scope of its business, and the sensitivity of the PII of the hundreds of millions of U.S. consumers that it obtains, stores, uses, transmits, sells, and manages. As alleged above, Equifax's security program and safeguards were not adequate to: identify reasonably foreseeable internal and external risks, assess the sufficiency of safeguards in place to control for these risks, or to detect, prevent, or respond to a data breach. In particular, Equifax's security program and safeguards were inadequate to evaluate and adjust to events that would have a material impact on Equifax's information security program, such as the numerous prior data breaches that other retailers and Equifax itself had experienced and the notification to Equifax that an identified vulnerability in a software program it utilized would make Equifax particularly susceptible to a data breach.

202. Equifax's duty to act reasonably in handling consumer data and to use reasonable data security measures also arises under Section 5 of the FTC Act, 15 U.S.C. §45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of not acting reasonably in the management of the data, and not using reasonable security measures to protect such data, by companies such as Equifax.

203. FTC guidelines, publications, and consent orders further form the basis of Equifax's duty and a corresponding reasonable standard of care.

204. In 2007, the FTC published guidelines which establish reasonable data security practices for businesses. The guidelines, which were updated in October 2016, note businesses

should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to identify a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.<sup>164</sup>

205. The FTC also has published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

206. And the FTC has issued orders against businesses that failed to employ reasonable measures to secure customer data. These orders provide further guidance to businesses with regard to their data security obligations.

207. In addition, individual states have enacted statutes based on the FTC Act and/or that otherwise require Equifax to act reasonably in the management of the data, and to use reasonable security measures to protect such data, as detailed herein, that also created a duty.

208. Equifax's duty to act reasonably in handling consumer data and to use reasonable data security measures also arises under the FCRA, 18 U.S.C. §1681, which regulates the collection, dissemination, and use of credit information. The FCRA explicitly recognizes a duty by Equifax, which is subject to the FCRA as a CRA as defined in 15 U.S.C. §§1681a(f) and (p),

---

<sup>164</sup> FTC, Protecting Personal Information: A Guide for Business (Oct. 2016), *available at*: [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf).



to maintain reasonable procedures in order to protect the confidentiality, accuracy and proper use of credit information, which includes the PII compromised in the Equifax Data Breach.

(b) Reasonable procedures

It is the purpose of this subchapter to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of this subchapter.

15 U.S.C. §1681.

209. As alleged in detail herein, Equifax's security practices and procedures were so severely deficient or nonexistent, despite its knowledge that this PII was coveted by attackers and certain to be subject to attempted hacks and exfiltration, that Equifax violated its duty to maintain reasonable procedures in order to protect the confidentiality, accuracy and proper use of credit information.

210. In fact, Equifax affirmatively assumed the duty to act with reasonable care in managing its data, and to use reasonable security measures to protect such data, as expressed in its public statements where it acknowledges that it is bound by the GLBA. In its privacy policies Equifax repeatedly states it uses "reasonable physical, technical and procedural safeguards to help protect" PII, which language is identical to that in the GLBA's Safeguards Rule. Through these and other statements alleged herein, Equifax specifically assumed the duty to comply with the data security industry standards that are applicable to a company whose sole business is transacting in PII. Plaintiff has alleged herein several industry standards of care with which Equifax has not complied.

211. In public statements, Equifax admits that it has an enormous responsibility to protect consumer PII, that it is entrusted with this data, and that it did not live up to its responsibility to protect PII.

212. A duty to act reasonably in the management of the data, and to use reasonable security measures to protect such data, also arises as a result of the special relationship that existed between Equifax and Plaintiff and the Class. This special relationship exists because financial institutions entrust credit bureaus like Equifax with customer PII and Equifax is in a unique position as one of only three nationwide credit reporting companies that serve as the linchpins of the financial system. Because of its crucial role within the credit system, Equifax was in a unique and superior position to protect against the harm suffered by Plaintiff and the Class as a result of the Equifax Data Breach. Indeed, **only** Equifax was in a position to ensure that its systems were sufficient to protect its primary asset – consumer PII.

213. Equifax breached its common law and statutory duties and industry standards of care – and was negligent – by actively mishandling the consumer data and failing to use reasonable measures to protect consumers’ personal and financial information from the hackers who perpetrated the Data Breach and by failing to provide timely notice of the Data Breach. Equifax mishandled its data management and IT systems by adopting and maintaining data security measures that Equifax knew or should have known were unreasonable and inadequate to protect PII. The specific affirmative negligent acts and omissions committed by Equifax include, but are not limited to, the following:

- a. Intentionally ignoring warnings about specific vulnerabilities in its systems identified by Equifax’s own employees, consultants, and software vendors;

- b. Maintaining (i) faulty patch management procedures, (ii) an insufficient firewall, (iii) feeble monitoring of endpoints and non-existent exfiltration monitoring, (iv) weak network segmentation, (v) inadequate monitoring and logging of network access, and (vi) insufficiently strict credentialing procedures that failed to restrict access to those with a valid purpose;
- c. Refusing to timely and adequately update security certificates on key systems;
- d. Storing and retaining PII in easily accessible systems rather than segregating it into locations with limited access and maximum security measures; and
- e. Failing to disclose the Data Breach in a timely manner.

214. As a result of the foregoing acts, Equifax breached its common law and statutory duties to act reasonably in the management of the data, and to use reasonable security measures to protect such data.

215. As a direct and proximate result of Equifax's negligent acts of misfeasance and nonfeasance, Plaintiff and the Class have suffered and continue to suffer injury and damages as described herein.

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests judgment in their favor and against Defendants for the relief set forth in their Prayer for Relief.

**COUNT 2**  
**Negligence Per Se**  
**(On behalf of Plaintiff and the Class)**

216. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

217. Equifax is a financial institution, as defined in Section 509(3)(A) of the GLBA, 15 U.S.C. §6809(3)(A).

218. Equifax has a duty to act reasonably in handling consumer data and to use reasonable data security measures that arises under the GLBA, 15 U.S.C. §§6801-6809, and its implementing regulations, 16 C.F.R. §314 (the “Safeguards Rule”), which “sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information” and “applies to the handling of customer information by all financial institutions[.]” 16 C.F.R. §314.1(a)-(b).

219. The Safeguards Rule “applies to all customer information in [a financial institution’s] possession, regardless of whether such information pertains to individuals with whom [a financial institution has] a customer relationship, or pertains to the customers of other financial institutions that have provided such information to [the subject financial institution].” 16 C.F.R. §314.1(b).

220. The Safeguards Rule requires financial institutions to “develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to [the financial institution’s] size and complexity, the nature and scope of [the financial institution’s] activities, and the sensitivity of any customer information at issue.” 16 C.F.R. §314.3(a).

221. Specifically, the Safeguards Rule requires a financial institution, among other things, to:

- (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could

result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

- (1) Employee training and management;
- (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
- (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

\* \* \*

(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program. 16 C.F.R. §314.4.

222. As alleged herein, Equifax breached its duties under the GLBA. The security program and safeguards Equifax maintained were not appropriate to Equifax's size and complexity, the nature and scope of its business, and the sensitivity of the PII of the hundreds of millions of U.S. consumers that it obtains, stores, uses, transmits, and manages. As alleged above, Equifax's security program and safeguards were not adequate to: identify reasonably foreseeable internal and external risks, assess the sufficiency of safeguards in place to control for these risks, or to detect, prevent, or respond to a data breach. In particular, Equifax's security program and safeguards were inadequate to evaluate and adjust to events that would have a material impact on Equifax's information security program, such as the numerous prior data breaches that other

retailers and Equifax itself had experienced and the notification to Equifax that an identified vulnerability in a software program it utilized would make Equifax particularly susceptible to a data breach.

223. Equifax’s violation of GLBA and the Safeguards Rule constitutes negligence per se.

224. The Safeguards Rule “applies to all customer information in [Equifax’s] possession, regardless of whether such information pertains to individuals with whom [it has] a customer relationship, or *pertains to the customers of other financial institutions [like Plaintiff and members of the Class] that have provided such information to [Equifax].*” 16 C.F.R. §314.1(b) (emphasis added). Plaintiff and the Class are “financial institutions” under the GLBA and therefore are expressly within the scope of persons the GLBA was intended to protect. Furthermore, Plaintiff and the Class are the entities that are required to reimburse consumers to the extent consumers’ financial accounts held with Plaintiff and the Class are impacted by identity theft or other fraudulent banking activity as a result of the Equifax Data Breach. Moreover, many of the class members are credit unions, which are organized as cooperatives whose members are consumers whose PII was compromised as a result of the Equifax Data Breach.

225. Furthermore, the harm that has occurred is the type of harm the GLBA was intended to guard against. Indeed, the FTC has pursued enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures, caused the same harm suffered by Plaintiff and the Class here.

226. Section 5 of the FTC Act, 15 U.S.C. §45, prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of not acting reasonably in the management of the data, and not using reasonable security measures to

protect such data. by companies such as Equifax. FTC guidelines, publications, and consent orders described above also form the basis of Equifax's duty. In addition, individual states have enacted statutes based on the FTC Act and/or that otherwise require Equifax to act reasonably in the management of the data, and to use reasonable security measures to protect such data, as detailed herein, that also created a duty.

227. Equifax violated Section 5 of the FTC Act (and similar state statutes) by mishandling consumer data and not using reasonable measures to protect PII and by not complying with applicable industry standards. Equifax's conduct was particularly unreasonable given the nature of the business conducted by Equifax and the vast amount of PII it obtained and stored and the foreseeable consequences of a data breach at a major credit reporting agency, including specifically the immense damages that would result to consumers and financial institutions.

228. Equifax mishandled its data management and IT systems by adopting and maintaining data security measures that Equifax knew or should have known were unreasonable and inadequate to protect PII. The specific affirmative negligent acts and omissions committed by Equifax include, but are not limited to, the following:

- a. Intentionally ignoring warnings about specific vulnerabilities in its systems identified by Equifax's own employees, consultants, and software vendors;
- b. Maintaining (i) faulty patch management procedures, (ii) an inadequate firewall, (iii) feeble monitoring of endpoint and non-existent exfiltration monitoring, (iv) weak network segmentation, (v) inadequate monitoring and logging of network access, and (vi) insufficiently strict credentialing procedures that failed to restrict access to those with a valid purpose;

- c. Refusing to timely and adequately update security certifications on key systems;
- d. Storing and retaining PII in easily accessible systems rather than segregating it into locations with limited access and maximum security measures; and
- e. Failing to disclose the Data Breach in a timely manner.

229. Equifax's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

230. Plaintiff and the Class are within the scope of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect as they are engaged in trade and commerce and bear primary responsibility for paying for and reimbursing consumers for fraud losses and other costs associated with the compromise of PII. Moreover, many of the class members are credit unions, which are organized as cooperatives whose members are consumers.

231. Furthermore, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same type of harm suffered by Plaintiff and the Class here.

232. As a direct and proximate result of Equifax's negligence per se, Plaintiff and the Class have suffered and continue to suffer injury and damages as described herein.

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests judgment in their favor and against Defendants for the relief set forth in their Prayer for Relief.



**COUNT 3**  
**Declaratory and Equitable Relief**  
**(On Behalf of the Plaintiff and the Class)**

233. Plaintiffs repeat and reallege each and every allegation contained above as if fully set forth herein.

234. Under Pennsylvania's Declaratory Judgment Act, 42 Pa. C.S.A. § 7531, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and that violate the terms of the federal and state statutes described in this complaint.

235. An actual controversy has arisen in the wake of Equifax's Data Breach regarding its common law and other duties to reasonably safeguard its customers' PII a. Plaintiffs allege that Equifax's data security measures were inadequate and remain inadequate. Equifax denies these allegations. Furthermore, Plaintiffs continue to suffer injury and damages as described herein.

236. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. Equifax continues to owe a legal duty to act reasonably in managing consumer data and to secure PII under, *inter alia*, the common law, GLBA, Section 5 of the FTC Act, the FCRA, and the state statutes alleged to herein;
- b. Equifax continues to breach its legal duty by actively mishandling consumer data and failing to employ reasonable measures to secure PII ; and
- c. Equifax's ongoing breaches of its legal duty continues to cause Plaintiff harm.

237. The Court should also issue corresponding injunctive relief requiring Equifax to employ adequate security protocols consistent with industry standards to protect PII. This injunction should direct Equifax to implement data security procedures, protocols, and measures that are in accordance with industry best practices and that are appropriate for the size and complexity of Equifax's business and the sensitivity of the PII it obtains, stores, uses, transmits and manages. More specifically, this injunction should, among other things, direct Equifax to:

- a. Implement procedures to provide for timely and proper patching of all servers with appropriate security-specific system patches;
- b. Implement procedures to timely and properly update security certificates
- c. Install an appropriate firewall;
- d. Implement strong network segmentation;
- e. Provide for sufficient logging and monitoring of network access, exfiltration monitoring, and whitelisting;
- f. Enhance endpoint and email security;
- g. Strengthen credentialing procedures and restrict access to PII to those with a valid purpose;
- h. Install all upgrades recommended by manufacturers of security software and firewalls used by Equifax;
- i. Engage third party auditors to test its systems for weakness and upgrade any such weakness found;
- j. Train and audit its data security personnel regarding any new or modified procedures and how to respond to a data breach; and

- k. Regularly test its systems for security vulnerabilities, consistent with industry standards, and upgrade any vulnerabilities identified.

238. If an injunction is not issued, Plaintiffs will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Equifax, which is a real possibility given the continued missteps taken by Equifax described herein, including using its official corporate communications to send affected consumers to phishing sites. Indeed, Equifax was hit with a separate data breach in March 2017 that apparently did nothing to motivate it to discover the other massive data breach going on at the same time.<sup>165</sup> The risk of another such breach is real, immediate, and substantial. If another breach at Equifax occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct. In particular, Plaintiff will be subject to reputational harm and the loss of goodwill resulting from the customer confusion and anxiety that will occur when another data breach and identity theft impacts them.

239. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Equifax if an injunction is issued. Among other things, if another massive data breach occurs at Equifax, Plaintiff and the Class have already incurred and will likely incur millions of dollars in damages and the credit reporting system on which Plaintiff and the Class rely could collapse. On the other hand, the cost to Equifax of complying with an injunction by employing reasonable data security measures is relatively minimal, and Equifax has a pre-existing legal obligation to employ such measures.

---

<sup>165</sup> Mark Coppock, *Equifax Confirms It Suffered A Separate Data Breach In March*, DIGITAL TRENDS (Oct. 3, 2017), <https://www.digitaltrends.com/computing/equifax-data-breach-affects-143-million-americans/>.

240. Issuance of the requested injunction will serve the public interest by preventing another data breach at Equifax, thus eliminating the injuries that would result to Plaintiffs, the Class, and the potentially millions of consumers whose confidential information would be compromised.

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests judgment in their favor and against Defendants for the relief set forth in their Prayer for Relief.

### **PRAYER FOR RELIEF**

Plaintiff, individually and on behalf of the Class respectfully request that the Court:

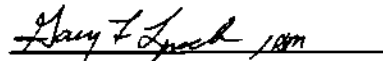
- A. Certify the Class and appoint Plaintiff and Plaintiff's counsel to represent the Class;
- B. Enter a monetary judgment in favor of Plaintiff and the Class to compensate them for the injuries they have suffered and will continue to suffer, together with pre-judgment and post-judgment interest and treble damages and penalties where appropriate;
- C. Enter a declaratory judgment as described herein and corresponding injunctive relief requiring Equifax to employ adequate data security protocols consistent with industry standards to protect PII;
- D. Grant the injunctive relief requested herein;
- E. Award Plaintiff and the Class reasonable attorneys' fees and costs of suit, as allowed by law; and
- F. Award such other and further relief as this Court may deem just and proper.

### **DEMAND FOR JURY TRIAL**

Plaintiffs demand a trial by jury on all claims so triable.

Dated: July 12, 2019

Respectfully Submitted,



Gary F. Lynch

Kelly K. Iverson

Jamison A. Etzel

**CARLSON LYNCH, LLP**

1133 Penn Avenue, 5th Floor

Pittsburgh, Pennsylvania 15222

Tel.: 412-322-9243

Fax: 412-231-0246

[glynch@carlsonlynch.com](mailto:glynch@carlsonlynch.com)

[kiverson@carlsonlynch.com](mailto:kiverson@carlsonlynch.com)

[jetzel@carlsonlynch.com](mailto:jetzel@carlsonlynch.com)

*(All to be admitted Pro Hac Vice)*

Joseph P. Guglielmo

Erin Green Comite

**SCOTT+SCOTT**

**ATTORNEYS AT LAW LLP**

230 Park Avenue, 17th Floor

New York, NY 10169

Tel.: 212-223-6444

Fax: 212-223-6334

[jguglielmo@scott-scott.com](mailto:jguglielmo@scott-scott.com)

[ecomite@scott-scott.com](mailto:ecomite@scott-scott.com)

**VERIFICATION**

The undersigned herein avers that the statements of fact contained in the foregoing are true and correct to the best of its information, knowledge and belief, and are made subject to penalties of 18 Pa. C.S.A. § 4904 relating to unsworn falsification to authorities.

Dated: July 12, 2019

FIRST CHOICE FEDERAL CREDIT UNION

By: Michael Muth

Title: CEO

